Red Teaming

Masterarbeit

zum Erlangen des akademischen Grades eines

Master of Science (M.Sc.)

IT-Sicherheitsmanagement

vorgelegt von

Jonathan Haist geb. Beißwenger

[redacted]

[redacted]

Mat.-Nr.: 73302

HTW Aalen

Hochschule für Technik und Wirtschaft

UNIVERSITY OF APPLIED SCIENCES

Erstgutachter: Prof. Roland Hellmann

Zweitgutachter: Prof. Dr. Christoph Karg

Ehrenwörtliche Erklärung

Ich versichere hiermit, dass ich meine Masterarbeit mit dem Thema *Red Teaming* selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

Aalen, 25.07.2019

Kurzfassung

Zu Beginn der Arbeit wurden die theoretischen Grundlagen zu Penetrationstest, Audit und Red Teaming beschrieben. In den rechtlichen Rahmenbedingungen wurden betroffene Gesetze unter die Lupe genommen. Dabei ist es wichtig, dass der durchgeführte Test vertraglich festgehalten wird und eine Einverständniserklärung vorliegt. Eine Abweichung von den vereinbarten Tests kann zur Strafbarkeit führen. Anschließend wurde eine Marktforschung bestehend aus einer Primär- und einer Sekundärmarkforschung durchgeführt. Die Sekundärforschung beschreibt die Angebote und Dienstleister, die auf dem Markt Red Teaming anbieten. Daraus wurden Unternehmen aus dem DACH-Raum für die Interviews der Primärforschung ausgewählt. In den Interviews kam heraus, dass es verschiedene Ausprägungen von Red Teaming gibt, die sich je Dienstleister, je Projekt und je Kunde unterscheiden können.

Die Ausprägungen lassen sich in die übergeordneten Kategorien „*bedrohungsbasiertes*“ und "*informations-/wissensbasiertes*" Red Teaming aufteilen. Beim bedrohungsbasierten Red Teaming werden Angriffe auf Grundlage der Bedrohungen eines Unternehmens durchgeführt. Im Gegensatz dazu basiert das "*informations-/wissensbasierte*“ Red Teaming auf Grundlage der gesammelten Informationen, den Anforderungen des Auftraggebers und der Expertise des Testteams.

Das Red Team muss ein vorher definiertes Ziel erreichen, das in der Regel die "Kronjuwelen", d. h. wichtige Prozesse, Systeme oder sensible Informationen sind. Das Red Team führt in Abstimmung mit dem White Team Angriffe durch, die technische, physische und menschliche Komponenten betreffen können. Welche Komponenten verwendet werden, unterscheidet sich nach Projekt und Dienstleister. Das Blue Team hat die Aufgabe, die Angriffe zu erkennen und darauf zu reagieren.

Mit dem gesammelten theoretischen Wissen und den Interviews wurden die Methoden verglichen und eine Methodik zur Einordnung erstellt. Das Red Teaming, Penetrationstests und Audits sind für unterschiedliche Situationen nützlich. Um die Auswahl zu erleichtern, ist es sinnvoll, die Ziele zu definieren, die mit dem Test erreicht werden sollen. Der Stand bzw. Reifegrad der Informationssicherheit kann ein hilfreicher Indikator sein, um sich für oder gegen ein Red Teaming zu entscheiden, da von vielen IT-Sicherheitsexperten empfohlen wird, den Sicherheitstest erst durchzuführen, wenn bereits gewisse Sicherheitsmaßnahmen umgesetzt wurden. Als dritter Indikator ist der Scope hilfreich, da ein Penetrationstest eine technische Prüfung darstellt und beim Audit oder Red Teaming oftmals eine ganzheitliche Betrachtung der Organisation erfolgt.

Im letzten Abschnitt wird eine praktikable Methode zur Durchführung von Red Teaming beschrieben. Hierzu wurden Thesen auf Grundlage des gesammelten Wissens aufgestellt.

Der Red Teaming Prozess kann in die Hauptprozesse Vorbereitung, Durchführung und Abschluss gegliedert werden. Für die Durchführung ist die Cyber Kill Chain von Lockheed

Martin, die Extended Cyber Kill Chain, die Unified Kill Chain und das MITRE ATT&CK-Framework hilfreich. Im Kapitel technische Umsetzung werden Angriffe aus den Bereichen physische, personelle und technische Sicherheit beschrieben.

Die Arbeit endet mit einem Fazit und den Zukunftsaussichten von Red Teaming.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

ACL	Access Control List
APT	Advanced Persistent Threats
ATT&CK	Adversarial Tactics, Techniques and Common Knowledge
AV	Antivirus
BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassung
BMWI	Bundesamt für Wirtschaft und Energie
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT	Blue Team
CERT	Computer Emergency Response Team
CIA	Vertraulichkeit (engl. confidentialtity), Integrität (eng. integrity), Verfügbarkeit (engl. availabilty)
CISO	Chief Information Security Officer
CREST	Council of Registered Ethical Security Testers
CSC	Cyber-Sicherheits-Check
DNS	Domain Name System
DS-GVO	Datenschutzgrundverordnung
EPK	Ereignisgesteuerte Prozesskette
GeschGehG	Gesetz zum Schutz von Geschäftsgeheimnissen
GG	Grundgesetz
GPDR	General Data Protection Regulation
GTL	Genereic Threat Landscape
HTTP/S	Hypertext Transfer Protocol / Secure
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IS	Informationssicherheit
ISACA	Information Systems Audit and Control Association
ISECOM	Institute for Security and Open Methodologies
ISMS	Informationssicherheitsmanagementsystem
ISO	International Organization for Standardization
IT	Informationstechnik
KMU	Kleine und mittlere Unternehmen
MITRE	Massachusetts Institute of Technology Research And Engineering
MoD	Ministry of Defence
NDA	Non-disclosure Agreement
NIST	National Institute of Standards and Technology
OSINT	Open Source Intelligence
OSSTMM	Open Source Security Testing Methodology Manual
OWASP	Open Web Application Security Project
PoC	Proof of Concept
PSS	Physical Security Systems Assessment Guide

RT	Red Team
SANS	SysAdmin, Networking and Security
SAP	Softwarehersteller (Systeme, Anwendungen und Produkte)
SGB	Sozialgesetzbuch
SOC	Security Operation Center
SQL	Datenbanksprache; Structured Query Language
StGB	Strafgesetzbuch
TCT	TIBER-Cyber-Team
TI	Threat Intelligence
TIBER	Threat Intelligence-based Ethical Red Teaming
TKC	TIBER-EU Knowledge Centre
TKG	Telekommunikationsgesetz
TTI	Targeted Threat Intelligence
TTP	Tactics, Techniques, Procedures
UKC	Unified Kill Chain
UMTS	Universal Mobile Telecommunications System
Urhg	Urheberrecht
URL	Uniform Resource Locator
UWG	Gesetz gegen den unlauteren Wettbewerb
WLAN	Wireless Local Area Network
WT	White Team
WTL	White Team Lead

1 Einleitung

Durch die wachsende Komplexität der Systeme und der fortschreitenden Vernetzung aller Bereiche der Informationsgesellschaft, nehmen die Risiken von Störungen sowie Angriffen von innen und außen zu. Die Bedrohungen haben eine hohe Dynamik und Cyber-Angriffe werden flexibler und professioneller. Durch die schnelle Entwicklung der IT-Systeme verändern sich auch die Angriffsmethoden ständig. Dies wurde im Bericht über die Lage der IT-Sicherheit in Deutschland im Jahr 2018 vom Bundesamt für Sicherheit in der Informationstechnik veröffentlicht.[1]

Um Finanzinfrastrukturen und -institutionen vor anspruchsvollen Cyberangriffen zu schützen, hat die Europäische Zentralbank im Mai 2018 ein *„Framework for Threat Intelligence-based Ethical Red Teaming“* (TIBER-EU) veröffentlicht. In diesem Framework wird die Vorgehensweise des Red Teamings beschrieben.[2]

Red Teaming ist eine spezifische Methode, bei dem zwei Teams gebildet werden. Das „*Red Team*“ übernimmt die Rolle des Angreifers und das „*Blue Team*“ ist für die Verteidigung zuständig. Diese Methode wird schon seit Jahrzehnten im Militärbereich erfolgreich eingesetzt und findet seit einigen Jahren auch im Zivilbereich seinen Gebrauch. Dabei geht es nicht nur um das Durchführen von physischen Angriffen. Die Methodik kann auch zum Beleuchten von theoretischen Fragestellungen aus verschiedenen Blickwinkeln und mit unterschiedlichen Schwerpunkten dienen.[3]

Auf der it-sa 2018, Europas größter und führender Fachmesse für IT-Sicherheit, wurden Vorträge zum Thema Red Teaming gehalten:

- Red Teaming: Fortgeschrittene Bedrohungsanalysen durch simulierte Angriffe[4]
- Red and Tiger Teaming: Erfahrungsbericht aus 8 Jahren Spionageüberprüfungen[5]
- Red Team Assessments: Durchführung professioneller Angriffssimulationen[6]

Auch im Magazin für professionelle Informationstechnik iX, wurde in diesem Jahr eine Reihe von Artikeln zum Thema Red Teaming veröffentlicht. Die komplette Artikelreihe ist im

[1] Vgl. *BSI*, Die Lage der IT-Sicherheit in Deutschland 2018, 2018, S. 3.
[2] Vgl. *ECB*, ECB publishes European framework for testing financial sector resilience to cyber attacks, 2018.
[3] Vgl. *Abolhassan, F.*, Security Einfach Machen, S. 32-33.
[4] Vgl. *Ott, K.*, Red Teaming: Fortgeschrittene Bedrohungsanalysen durch simulierte Angriffe, 2018.
[5] Vgl. *Hackner, T.*, Red and Tiger Teaming: Erfahrungsbericht aus 8 Jahren Spionageüberprüfungen, 2018.
[6] Vgl. *Herzog, S.*, Red Team Assessments: Durchführung professioneller Angriffssimulationen, 2018.

Sonderheft IT-Sicherheit zu finden.[7] Das Thema bekommt in der Branche aktuell einen immer größeren Stellenwert und wird von vielen Unternehmen praktiziert.

1.1 Quellen, Methoden, Ziele

Das BSI stellt umfangreiche Informationen zum Thema Penetrationstests zur Verfügung. Beispielsweise wird eine Studie „*Durchführungskonzept für Penetrationstests*“ oder ein „*Praxis-Leitfaden für IS-Penetrationstests*“ bereitgestellt.[8] Des Weiteren gibt es vom National Institute of Standards and Technology (NIST) einen „*Technical Guide to Information Security Texting and Assessment*“.[9] Weitere Informationen werden aus dem Open Web Application Security Project (OWASP) entnommen, wie bspw. dem OWASP Testing Guide.[10] Das Open Source Security Testing Methodology Manual (OSSTMM) vom Institute for Security and Open Methodologies (ISECOM) wird ebenfalls betrachtet.[11] Die Standards und Methoden wurden entwickelt, um Penetrationstests transparenter zu machen.

In dieser Masterarbeit soll eine praktikable Methode zur Anwendung von Red Teaming entwickelt werden. Hierfür wird das TIBER-EU Rahmenwerk hinzugezogen und kritisch hinterfragt. Ebenso wird das im Jahr 2003 vom SANS Institute veröffentlichte Paper „*Red Teaming: The Art of Ethical Hacking*“ auf Aktualität geprüft.[12] Weitere Daten werden durch Interviews und Umfragen bei Unternehmen gewonnen, die bereits einen derartigen Test durchgeführt haben. Durch die Recherche soll herausgearbeitet werden, wie sich ein Red Teaming von klassischen Penetrationstests und Audits unterscheidet, welche Vor- und Nachteile vorhanden sind und welche Risiken entstehen können. Auch juristische Grundlagen sollen geprüft werden.

Auf dem Markt gibt es bereits Dienstleister die Red Teaming durchführen. Diese Angebote werden untersucht und verglichen.

Die grundlegende Fragestellung, die mit der Arbeit beantwortet werden soll, ist, welchen Nutzen ein Red Teaming für den Kunden hat, bzw. wie sinnvoll es ist, einen Test durchzuführen.

- Was zeichnet Red Teaming im Vergleich zu bestehenden und beschriebenen Methoden aus? Welche Definition ist sinnvoll?
- Was ist ein methodisch und juristisch vertretbarer Weg, ein Red Teaming in einem Unternehmen durchzuführen?

[7] Vgl. *IX-REDAKTION*, iX Kompakt (2019) IT-Sicherheit.
[8] Vgl. *BSI*, Studie Durchführungskonzept für Penetrationstests.
[9] Vgl. *Scarfone, K. A.* u. a., Technical guide to information security testing and assessment.
[10] Vgl. *OWASP*, OWASP Testing Guide v4 Table of Contents.
[11] Vgl. *Herzog, P.*, Open Source Security Testing Methodology Manual (OSSTMM).
[12] Vgl. *Peake, C.*, Red Teaming: The Art of Ethical Hacking, 2003.

2 Theoretische Grundlagen

In diesem Kapitel werden die für die Masterarbeit relevanten theoretischen Grundlagen erläutert. Wenn mehrere Unterkapitel vorhanden sind, wird das Kapitel durch ein Fazit ergänzt.

2.1 Cyber-Sicherheit, Informationssicherheit, IT-Sicherheit

Die Aufgabe von IT-Sicherheit (engl. IT-Security) ist das Unternehmen und deren Werte (z. B. Know-how, Kundendaten, Personaldaten) zu schützen und wirtschaftliche Schäden, die durch Vertraulichkeitsverletzungen, Manipulation oder Störungen entstehen können, zu verhindern. Eine vollständige Vermeidung oder Verhinderung von Angriffen ist nicht möglich, daher umfasst das Gebiet der IT-Sicherheit insbesondere Maßnahmen und Konzepte, um das Ausmaß potenzieller Schäden, die durch Sicherheitsvorfälle entstehen können, zu reduzieren und die Risiken zu verringern.[13] Dabei beschäftigt sich IT-Sicherheit mit dem Schutz elektronisch gespeicherter Informationen und deren Verarbeitung. Informationssicherheit hingegen hat den Schutz von Informationen als Ziel, wozu beispielsweise Informationen auf Papier, in Rechnern oder in Köpfen gespeichert zählen können. Die Informationssicherheit ist daher umfassender als IT-Sicherheit.[14]

Weitere Eigenschaften, die häufig in Zusammenhang mit IT-Sicherheit stehen, werden in folgender Tabelle erläutert.

Tabelle 1: Begriffsdefinitionen[15]

Eigenschaft	Definition
Funktionssicherheit (engl. safety)	Die Funktionssicherheit beschreibt die Eigenschaft, dass eine realisierte Ist- mit der spezifizierten Soll-Funktionalität übereinstimmt.
Informationssicherheit (engl. security)	Die Informationssicherheit beschreibt die Eigenschaft nur solche Systemzustände anzunehmen, die zu keiner unautorisierten Informationsveränderung oder -gewinnung führen kann.
Datensicherheit (engl. protection)	Die Datensicherheit ist ein Teilgebiet der Informationssicherheit. Die Datensicherheit beschreibt die Eigenschaft, dass nur autorisierter Zugriff auf Systemressourcen und insbesondere auf Daten zugelassen wird. Dies umfasst insbesondere Maßnahmen zur Datensicherung, um vor Datenverlust durch die Erstellung von Sicherungskopien zu schützen.

[13] Vgl. *Eckert, C.*, IT-Sicherheit, 2018, S. 1.
[14] *BSI*, Glossar - IT-Grundschutz-Kataloge.
[15] Vgl. *Eckert, C.*, IT-Sicherheit, 2018, S. 6, 14

Eigenschaft	Definition
Datenschutz (engl. Privacy / data protection)	Der Datenschutz ist eine Eigenschaft der Informationssicherheit. Er wird durch das Bundesdatenschutzgesetz (BDSG) und die EU-Datenschutzgrundverordnung (DS-GVO; engl. General Data Protection Regulation (GPDR)) geregelt. Die Gesetze bieten Schutz für die persönlichen Daten natürlicher Personen. In diesen Bereich fallen insbesondere Sicherheitsanforderungen, die der deutsche Gesetzgeber durch das informationelle Selbstbestimmungsrecht geregelt hat. Das Recht auf informationelle Selbstbestimmung (Artikel 1 Absatz 1 GG) ist ein Grundrecht, das jedem Bürger der Bundesrepublik Deutschland durch das Grundgesetz (GG) eingeräumt wird.[16] Das Grundrecht gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

Funktionssicherheit (engl. safety) und Informationssicherheit (engl. security) grenzt zwei verschiedene Aspekte von IT-Sicherheit ein. Bei Funktionssicherheit geht es um die Zuverlässigkeit bzw. Funktionalität von einem System, insbesondere dessen Ablauf- und Ausfallsicherheit. Informationssicherheit hingegen bezeichnet den Schutz eines Systems vor beabsichtigten Angriffen. Die Begriffe sind nicht unabhängig voneinander, die Funktionssicherheit schließt vielmehr die Informationssicherheit mit ein.[17]

Der Begriff Cyber geht auf den Begriff Cybernetics (dt. Kybernetik) zurück. Hiermit ist die Kunst des Steuerns im Sinne der Automatisierung von Prozessen und Systemen gemeint.[18] Unter dem Begriff Cyber-Sicherheit (engl. Cyber-Security) werden die Herausforderungen in Bezug auf IT-Sicherheit zusammengefasst, die sich aus der Vernetzung von IT-Systemen und den zunehmenden Abhängigkeiten von vernetzten, sicherheitskritischen Infrastrukturen ergeben.[19] Das Aktionsfeld der klassischen IT-Sicherheit wird auf den gesamten Cyber-Raum ausgeweitet.[20] Als Cyber-Raum wird die Gesamtheit der IT-Infrastruktur in Unternehmen, Behörden, oder aber auch in Produktionsanlagen, im Gesundheitswesen, im Finanzbereich und der Logistik, die über das Internet oder vergleichbare Vernetzungstechnologien zugreifbar sind, bezeichnet.[21]

Die Unterscheidung zwischen Cyber- und IT-Sicherheit kann anhand der Maßnahmen abgeleitet werden. Die IT-Sicherheit umfasst die technischen Maßnahmen zum Schutz der Netzwerke, der Computersysteme und der dazugehörigen Software vor bereits bekannten

[16] Vgl. *Datenschutz.org*, Datenschutz in Deutschland & der Europäischen Union, 2019.
[17] Vgl. *Sikora, A.*, Security im Überblick (Teil 1): Einführung in die Kryptographie, 2003.
[18] Vgl. *Bartsch, M./Frey, S.*, Cyberstrategien für Unternehmen und Behörden, 2017, S. 8.
[19] Vgl. *Eckert, C.*, IT-Sicherheit, 2018, S. 44.
[20] Vgl. *BSI*, Cyber-Sicherheit, 2019.
[21] Vgl. *Eckert, C.*, IT-Sicherheit, 2018, S. 44

Angriffen. Die Cyber-Sicherheit umfasst hingegen alle Maßnahmen der jeweiligen Organisation zum Schutz vor Angriffen, die durch oder mit Computersystemen durchgeführt werden und einen Schaden beim Zielsystem erzeugen können. Im Vergleich zur IT-Sicherheit ist die Cyber-Sicherheit komplexer und schließt auch nicht-technische Aspekte, wie organisatorische, physische und personelle Aspekte mit ein. Die IT-Sicherheit ist Teil der Cyber-Sicherheit.[22]

Die Begriffe sind nicht genormt und können daher unterschiedlich definiert werden. Die genannten Unterschiede zwischen Cyber-Sicherheit, Informationssicherheit und IT-Sicherheit sind für viele nicht praktisch relevant und werden daher häufig gleichbedeutend verwendet.[23] In dieser Arbeit werden die Begriffe wie folgt verwendet:

- IT-Sicherheit: technische Maßnahmen zum Schutz der Informationen.
- Informationssicherheit: alle Maßnahmen zum Schutz von Informationen.
- Cyber-Sicherheit: alle Maßnahmen zum Schutz von Informationen über Netzgrenzen hinweg.

2.2 Schutzziele

Informationssicherheit befasst sich mit dem Schutz von Informationen. Die Schutzziele präzisieren diese Anforderung. In folgender Übersicht werden die gängigen Schutzziele von Organisationen erläutert.

Tabelle 2: Schutzziele[24]

Schutzziel	Beschreibung
Vertraulichkeit (engl. confidentialtity)	Informationen sind nur für Berechtigte zugreifbar.
Integrität (engl. integrity)	Genauigkeit, Korrektheit und Vollständigkeit von Informationen und Verfahren (Validität). Die Daten werden nicht unberechtigt verändert, gelöscht oder zerstört.
Verfügbarkeit (engl. availability)	Objekte sind bei Bedarf für Berechtigte zugreifbar und nutzbar.
Verbindlichkeit (engl. liability) / Zuordenbarkeit / Nichtabstreitbarkeit (engl. non repudiation) / Authentizität	Zurechenbare (nicht rückweisbare), rechtsverbindliche Kommunikation. Die Grundlage für die Verbindlichkeit ist die Authentizität, d. h. ein Subjekt oder Objekt ist echt und entspricht den Behauptungen.

Als die drei Grundwerte der Informationssicherheit wird die Vertraulichkeit (engl. **c**onfidentiality), die Integrität (eng. **i**ntegrity) und die Verfügbarkeit (engl. **a**vailabilty)

[22] Vgl. *Bartsch, M./Frey, S.*, Cyberstrategien für Unternehmen und Behörden, 2017, S. 8.
[23] Vgl. *Hellmann, R.*, IT-Sicherheit, 2018, S. 2
[24] *Pohl, H.*, Taxonomie und Modellbildung in der Informationssicherheit, 2004., S. 679-680.

gesehen.[25] Aufgrund der Anfangsbuchstaben der englischen Bezeichnungen der Schutzziele wird in diesem Zusammenhang auch von CIA gesprochen.

2.3 Bedrohung, Schwachstelle und Risiko

Im englischen Sprachgebrauch wird bei einer Schwachstelle zwischen einer Schwäche (engl. weakness) und einer Verwundbarkeit (engl. vulnerability) eines Systems unterschieden. Die Schwäche von einem System kann zu einer Verwundbarkeit führen. Eine Verwundbarkeit ist eine Schwachstelle, die ausgenutzt werden kann, d. h. ein Dienst eines Systems kann umgangen, getäuscht oder unautorisiert modifiziert werden. Im deutschen Sprachgebrauch wird eine solche Unterscheindung in der Regel nicht getroffen. Eine Schwachstelle wird als eine Verwundbarkeit eines Systems gesehen. Das Ausnutzen von Schwachstellen beeinträchtigt die im Kapitel 2.2 definierten Schutzziele.

Eine Bedrohung (engl. threat) zielt darauf ab, eine oder mehrere Schwachstellen auszunutzen, um ein Schutzziel (siehe Kapitel 2.2) zu gefährden. Wenn die Bedrohung auf eine Schwachstelle trifft, wird von einer Gefährdung gesprochen, da durch die Bedrohung einer Schwachstelle die Gefahr besteht, dass diese ausgenutzt wird.

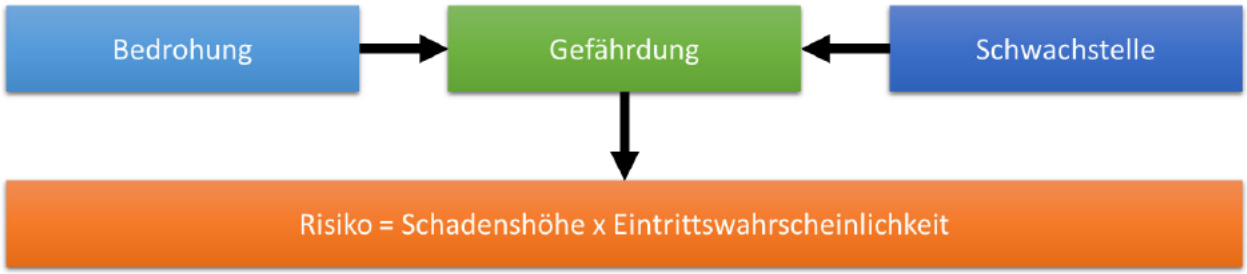
Das Risiko (engl. risk) einer Bedrohung besteht aus der Wahrscheinlichkeit des Eintritts eines Schadensereignisses und der Höhe des potenziellen Schadens, der dadurch hervorgerufen werden kann.[26] Durch das Risiko kann ein Schadenszenario bewertet und die Relevanz einer Schwachstelle bestimmt werden. Die erfassten Bedrohungen aus einer Bedrohungsanalyse und die bekannten Schwachstellen können als Grundlage für die Risikoanalyse (engl. risk assessment) und Bewertung der Risiken verwendet werden. Die Wahrscheinlichkeit für das Eintreten und der potenzielle Schaden, der dadurch verursacht werden kann, sind in der Regel nicht messbar und werden geschätzt. Ein quantitativer Wert für ein Risiko kann anhand folgender Formel berechnet werden.

Risiko (R) = Schadenshöhe (S) X Eintrittswahrscheinlichkeit (E)

Mit folgender Abbildung kann der Zusammenhang zwischen einer Schwachstelle, einer Bedrohung und einem Risiko verdeutlicht werden.

[25] *BSI*, Glossar - IT-Grundschutz-Kataloge.
[26] Vgl. *Eckert, C.*, IT-Sicherheit, 2018, S. 16-18, 197, 204.

Abbildung 1: Zusammenhang Schwachstelle, Bedrohung und Risiko



Das European Union Agency for Network and Information Security (ENISA) ist das Kompetenzcenter für Netz- und Informationssicherheit für die EU. In einem jährlichen Threat Landscape Report werden die TOP 15 Cyber-Bedrohungen und Trends veröffentlicht. Das Ranking wurde auf Grundlage von öffentlich zugänglichen Quellen und weiteren kommerziellen Anbietern erstellt. Das Ranking spiegelt die Häufigkeit des Auftretens der Bedrohung im Berichtszeitraum wieder. Die fünf häufigsten Bedrohungen werden in der Tabelle 3: ENISA TOP 5 Bedrohungen beschrieben.

Tabelle 3: ENISA TOP 5 Bedrohungen[27]

Bedrohung	Kurze Beschreibung
1. Malware (dt. Schadprogramme)	Die Schadprogramme sind die am häufigsten auftretende Cyber-Bedrohung. Jene entwickeln sich ständig weiter, um die Gewinne und Effektivitätsrate der Angreifer zu maximieren (siehe Kapitel 2.5).
2. Web Based Attacks (dt. Webbasierte Angriffe)	Webbasierte Angriffe haben Webserver und -dienste als Ziel. Webbasierte Angriffe zählen als eine der häufigsten Bedrohungen, da das Web eine große Angriffsfläche bietet. Es wird erwartet, dass die Bedrohungen zunehmen, da immer mehr Malware und Exploits auf das Web angewiesen sind.
3. Web Application Attacks (dt. Webanwendungsangriffe)	Ein Webanwendungsangriff ist ein Angriff auf Komponenten einer über das Web verfügbaren Software. Diese Angriffe überschneiden sich mit webbasierten Angriffen. Webanwendungen werden ein für Angreifer immer interessanteres Ziel, da immer mehr Firmen von Webservices in Bezug auf Umsatz und Reputation abhängig werden.
4. Phishing	Beim Phishing wird versucht, den Empfänger einer Phishing-E-Mail oder Nachricht dazu zu bringen einen bösartigen Anhang zu öffnen oder eine URL anzuklicken. Über diesen Weg werden z. B. Anmeldinformationen gestohlen. Phishing ist der bevorzugte Weg, Organisationen zu kompromittieren.

[27] Vgl. *ENISA*, ENISA Threat Landscape Report 2018, 2019, S. 24 ff.

Bedrohung	Kurze Beschreibung
5. Denial of Service (dt. Verweigerung des Dienstes)	(Distributed) Denial of Service (DoS) ist eine höchst wirkungsvolle Bedrohung, die sich an fast jede Organisation richtet. Der Angriff zielt darauf ab, die Verfügbarkeit von einem Dienst zu beeinträchtigen. Es gibt eine große Nachfrage nach DoS Mitigation Services und laut Statistik nehmen die DDoS-Aktivitäten zu.

2.4 Angriff, Angreifer und Angriffsvektor

Ein Angriff (engl. attack) ist ein nicht autorisierter Zugriff bzw. Zugriffsversuch auf ein System. Bei einem Angriff wird versucht, eine Schwachstelle auszunutzen. Hierbei kann eine Unterscheidung zwischen einem passiven und aktiven Angriff getroffen werden.

Passive Angriffe betreffen die unautorisierte Informationsgewinnung und zielen auf den Verlust der Vertraulichkeit ab, z. B. durch das Abhören von einer Kommunikationsverbindung (engl. sniffing) oder das unautorisierte lesen von Dateien.

Aktive Angriffe betreffen die unautorisierte Modifikation von Datenobjekten und richten sich gegen die Integrität oder Verfügbarkeit des IT-Systems. Bei einem aktiven Angriff werden beispielsweise Pakete von einer Kommunikationsverbindung entfernt, eine falsche Identität vorgespielt (engl. Spoofing) oder ein Dienst lahmgelegt (engl. Denial-of-Service).[28]

Bei einem Angreifer wird in den Medien häufig von einem Hacker gesprochen. Darunter versteht man technisch sehr versierte Personen mit dem Ziel, Schwachstellen in IT-Systemen aufzudecken und Software zum Ausnutzen von Schwachstellen zu entwickeln. Die Hacker wenden sich an die Öffentlichkeit oder an Organisationen, um auf Schwachstellen aufmerksam zu machen. Bei Hackern, die keine persönlichen Vorteile wie finanzielle Gewinne oder bewusste wirtschaftliche Schäden Dritter zum Ziel haben, wird auch von Ethical Hacker gesprochen. Hacker, die gezielt zum eigenen Vorteil oder Nachteil eines Dritten Angriffe durchführen, werden als Cracker bezeichnet. Im Sprachgebrauch findet diese Unterscheidung nur selten statt. Cracker mit internem Wissen über eine Organisation werden auch als Insider bezeichnet.[29] In dieser Arbeit wird Hacker und Cracker synonym verwendet.

Im ENISA Threat Landscape Report 2018 wird von sieben Threat Agent Groups (dt. Bedrohungsklassen) gesprochen: [30]

- Cyber-criminals (dt. Cyber-Kriminelle)
- Nation States (dt. Nationale Staaten)
- Corporations (dt. Korporationen)

[28] Vgl. *Eckert, C.*, IT-Sicherheit, 2018, S. 19.
[29] Vgl. *Eckert, C.*, IT-Sicherheit, 2018, S. 22-23.
[30] Vgl. *ENISA*, ENISA Threat Landscape Report 2018, 2019, S. 118-123.

- Hacktivists (dt. Hacktivisten)
- Cyber Fighters / Cyber Terrorists (dt. Cyber Kämpfer / Cyber Terroristen)
- Script Kiddies

Um Fähigkeiten, Böswilligkeit, Motivation und Methoden der Angreifer herauszufinden, wurde die Tabelle aus dem Buch „*Cyber Warfare – Its Implications on National Security*" übersetzt und übernommen. Die Kategorien bzw. Begrifflichkeiten Cyber-Criminals und Corporations werden dort nicht beschrieben. Aufgrund der Beschreibung im ENISA-Report kann davon ausgegangen werden, dass die Beschreibung der Cyber-Criminals mit Black Hat Crackers gleichzusetzen sind. Corporations nutzen laut ENISA die gleichen Techniken wie die Bedrohungsklasse Nation States.[31]

Tabelle 4: Bedrohungsklassen[32]

Bedrohungs-klasse	Fähigkeiten	Böswilligkeit	Motivation	Methoden
Script Kiddies	sehr gering	gering	Langeweile, Fähigkeitssuche	Herunterladen und Ausführen von Hacking Scripts (Toolkits) und Exploits.
Hacktivists	gering	moderat	Unterstützung einer politischen Sache	Denial-of-Service-Angriffe oder Verunstaltung rivalisierter Webseiten.
Insider	Moderate	Hoch	Verärgerung, persönlicher Gewinn, Rache	Nutzt Insider Berechtigung-en, um den aktuellen oder ehemaligen Arbeitgeber anzugreifen.
Black hat cracker / Cyber-criminals	Sehr hoch	Sehr hoch	Persönlicher Gewinn, Gier, Rache	Ausgeklügelte Angriffe von Kriminellen/ Dieben; können in Crime-as-a-Service oder in die organisierte Kriminalität verwickelt sein.

[31] Vgl. *ENISA*, ENISA Threat Landscape Report 2018, 2019, S. 121.
[32] Vgl. *Relia, S.*, Cyber warfare, 2015, Amazon Kindle Table 4: Classification of Cyber Adversaries.

Bedrohungs-klasse	Fähigkeiten	Böswilligkeit	Motivation	Methoden
Cyber Terrorists	Sehr hoch	Sehr hoch	Politik, Spionage der Staatspolitik	Fundierte Cyber-Angriffe auf Zielländer
Nation States/ Corporations	Extrem hoch	Extrem hoch	Teil der nationalen Politik	regelrechter Cyberkrieg

Im ENISA Thread Landscape wird beschrieben, dass der dominierende Angriffsvektor für Malware Infektion kompromittierte E-Mails (Phishing, Spam und Spear-Phishing) sind. Laut Statistik werden zu 92,4% die E-Mail, zu 6,3% das Web und Browser und zu 1,3% andere Angriffsvektoren für die Malwareinfektion genutzt.[33]

In der jährlichen Bitkom Studie „*Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz in der Industrie*“ wurden 503 nach Branchen und Größenklassen repräsentativ ausgewählte Industrieunternehmen mit mindestens zehn Mitarbeitern befragt.[34]

Abbildung 2: Täterkreis

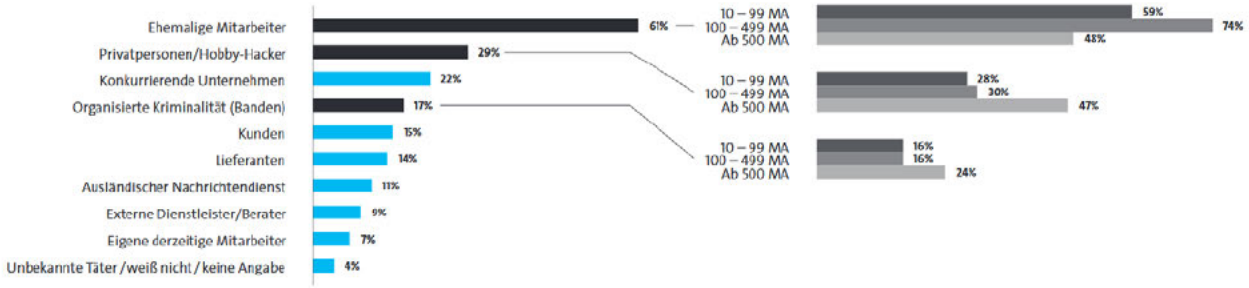


Abbildung 11: Täterkreis
Von welchem Täterkreis gingen diese Handlungen (vermutlich) in den letzten 2 Jahren aus?
Basis: Alle befragten Industrieunternehmen, die in den letzten 2 Jahren von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (n=343) | Mehrfachnennungen in Prozent
Quelle: Bitkom Research

Die Zahlen der Abbildung veranschaulichen, dass 68% der Delikte von Innentätern (Ehemalige Mitarbeiter 61%, Eigene derzeitige Mitarbeiter 7%) durchgeführt wurden. 60% der Delikte kommen aus dem unternehmerischen Umfeld (konkurrierende Unternehmen 22 %, Kunden 15%, Lieferanten 14%, externe Dienstleister / Berater 9%) und zu den weiteren Gruppen gehören Privatpersonen / Hobby-Hacker (29%), die organisierte Kriminalität (Banden) (17%) und ausländische Nachrichtendienste (11%).

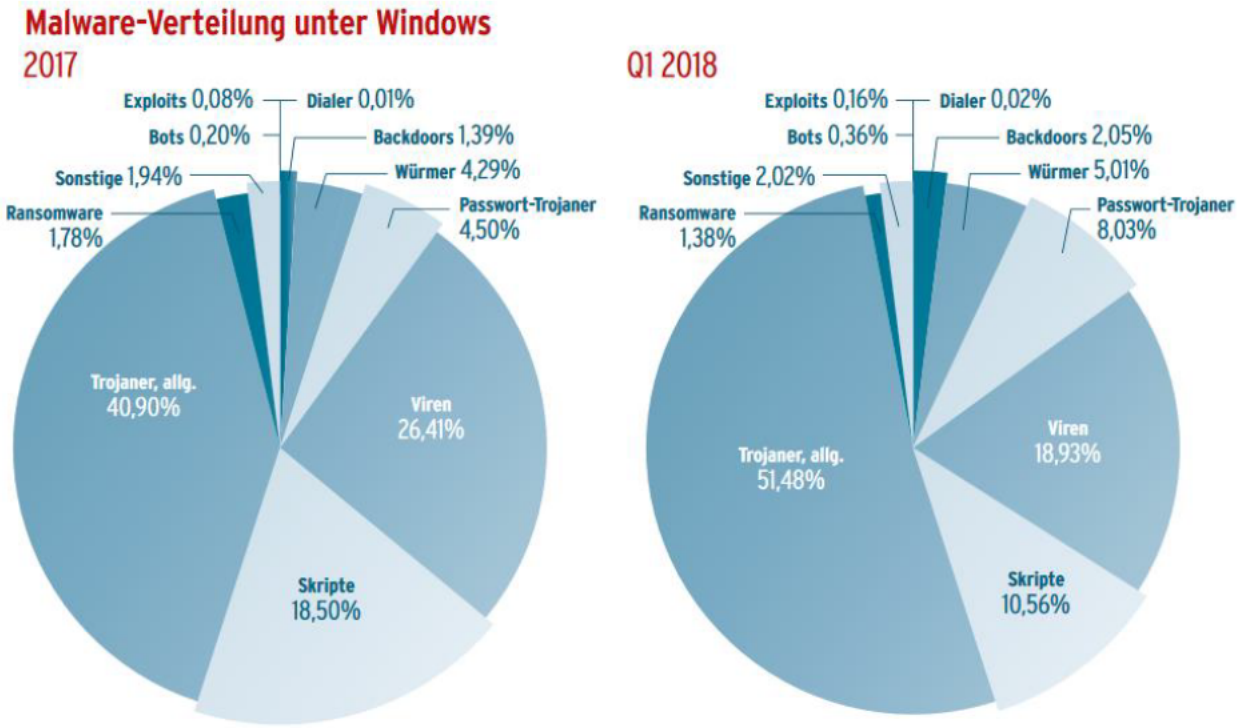
2.5 Malware, Exploit und APT

Der Begriff Malware ist ein Kofferwort, dass sich aus den englischen Wörtern **mal**icious (dt. bösartig) und soft**ware** zusammensetzt. Im deutschen Sprachgebrauch spricht man von Schadsoftware oder Schadprogramm.[35] Aus der folgenden Statistik (siehe Abbildung 3:

[33] Vgl. *ENISA*, ENISA Threat Landscape Report 2018, 2019, S. 31.
[34] Vgl. *Bitkom e.V.*, Spionage, Sabotage und Datendiebstahl - Wirtschaftsschutz in der Industrie., S. 28.
[35] *o. V.*, Schadprogramm, 2019.

Malware Verteilung unter Windows) kann abgelesen werden, dass der Großteil der Malware für Windows, Trojaner, Viren und schädliche Skripte sind.

Abbildung 3: Malware Verteilung unter Windows[36]



Es gibt eine unbeschränkte Bandbreite an Schadprogrammen. Im Folgenden werden die wichtigsten Typen kurz beschrieben. Die Übergänge zwischen den Typen sind hierbei fließend und es gibt sehr unterschiedliche Ausprägungen.

Tabelle 5: Schadprogramme[37]

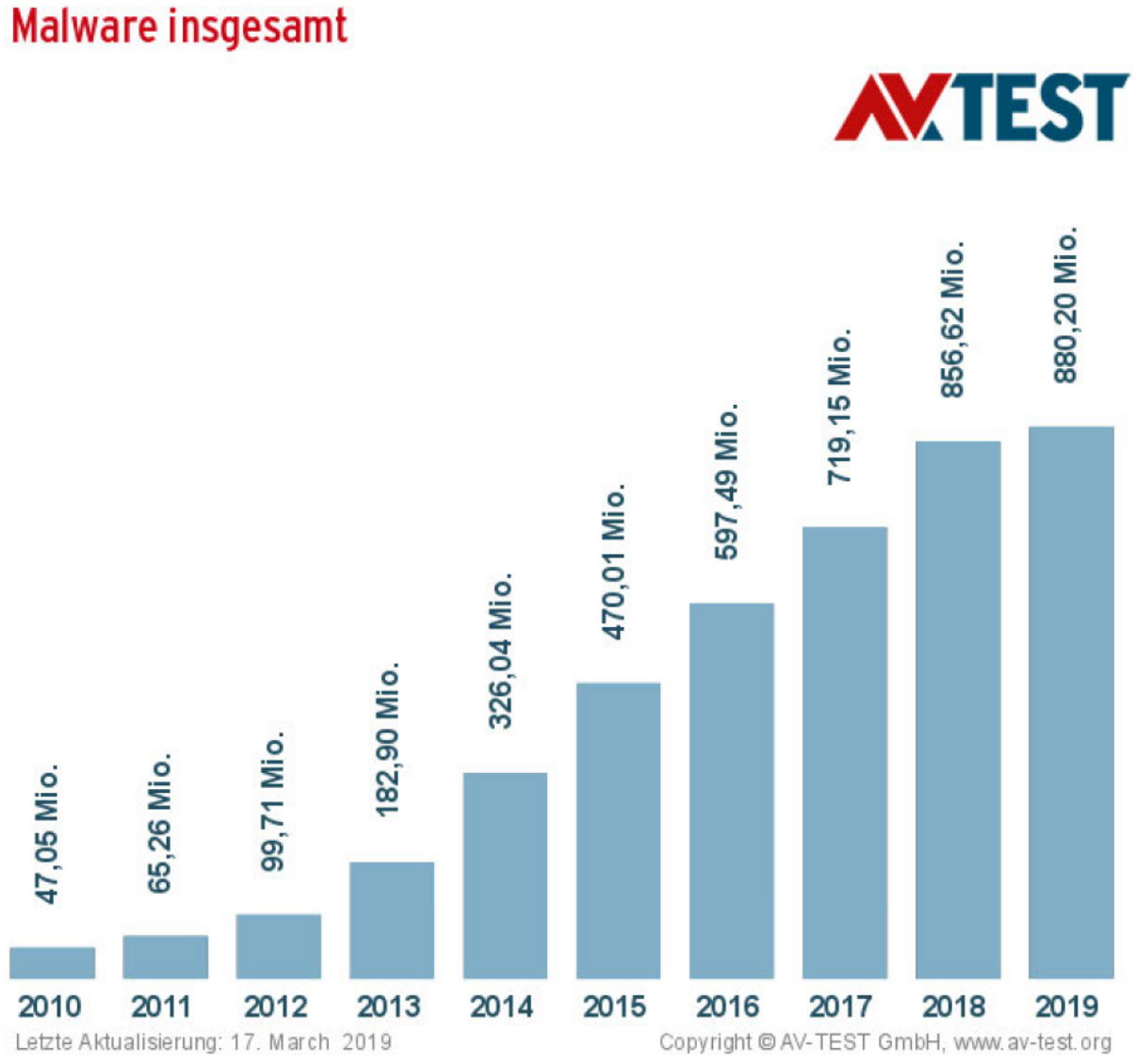
Schadprogramm	Beschreibung
Viren	Viren sind Programme, die an sich erlaubte Operationen, z. B. des Betriebssystems, zweckentfremden, um sich selbst zu verbreiten. Dazu hängen sie Kopien von sich an Programme oder Dokumente an. Evtl. werden Teile davon überschrieben. Das Ganze geschieht, ohne dass der Benutzer das möchte, und oft auch, ohne dass er es zunächst bemerkt.
Würmer	Unter Würmern versteht man, wie schon bei den Viren, ebenfalls Programme, die sich selbst verbreiten. Das geschieht allerdings anders als bei Viren dadurch, dass sie Sicherheitslücken in Software ausnutzen (...) Der Wurm schlüpft also sozusagen durch ein (Sicherheits-)Loch, daher der Name. Es werden im Gegensatz zu Viren Funktionalitäten verwendet, die so nicht vorgesehen sind. Außerdem erfolgt die Verbreitung meist aktiv über Netzwerkverbindungen eines lokalen Netzwerks oder des Internets.

[36] *AV-Test GmbH*, AV-TEST Sicherheitsreport 2017/2018: Die aktuelle Analyse zur IT-Bedrohungslage, 2018.
[37] *Hellmann, R.*, IT-Sicherheit, 2018, S. 119.

Schadprogramm	Beschreibung
Trojanisches Pferd / Trojaner	Dabei handelt es sich um Programme, die neben der vorgeblichen und erwünschten Funktion auch verborgene Funktionalitäten aufweisen. Das kann z. B. ein Tool sein, das angeblich den Rechner schneller macht, aber nebenbei späht es Passwörter aus und übermittelt sie ins Internet.

Das unabhängige IT-Security Institut AV-TEST GmbH registriert täglich mehr als 350.000 neue Schadprogramme (siehe Abbildung 4: Malware Statistik). Die Anzahl an Malware insgesamt steigt stetig an. Die Unternehmen sind einer steigenden Bedrohung von Malware ausgesetzt.

Abbildung 4: Malware Statistik[38]



[38] *AV-Test GmbH*, Malware.

Im Zusammenhang mit Schadprogrammen spricht man auch von Exploits. Diese zeigen Sicherheitslücken von Software auf und ermöglichen die Ausnutzung einer Schwachstelle. Sie werden von Angreifern als Werkzeug verwendet, um in ein Computersystem einzudringen und es zu manipulieren.[39] Ein Exploit kann von vielen unterschiedlichen Schadprogrammen verwendet werden. Von einem Exploit werden Payloads verwendet, dies sind Schadfunktionen, die sofort oder durch einen bestimmen Auslöser ausgeführt werden.[40]

Das BSI spricht aktuell im Bericht der Lage der IT-Sicherheit von einer steigenden Anzahl von sogenannten Advanced Persistent Threats (APT). Dabei handelt es sich um zielgerichtete Angriffe auf ausgewählte Institutionen, bei denen sich ein Angreifer persistenten/ dauerhaften Zugriff zu einem Netzwerk verschafft und diesen in der Folge auf weitere Systeme ausweitet. Die Angriffe zeichnen sich durch einen sehr hohen Ressourceneinsatz und erhebliche technische Fähigkeiten aufseiten der Angreifer aus und sind in der Regel schwierig zu detektieren.[41]

Ein Vergleich von traditionellen mit APT-Angriffen kann folgender Tabelle entnommen werden.

Tabelle 6: Vergleich traditioneller mit APT-Angriff[42]

	Traditioneller Angriff	APT-Angriff
Angreifer	meistens Einzelpersonen	organisierte, zielgerichtete und leistungsfähige Gruppe
Ziel	unspezifiziert, meistens individuelle Systeme	staatliche Institutionen, Wirtschaftsunternehmen
Zweck	finanzielle Vorteile, Beweis einer Fähigkeit	Wettbewerbsvorteile, strategische Vorteile
Ansatz	Einzellauf „Smash and Grab“, kurzfristig	wiederholte Versuche, bleibt leise und langsam, passt sich Schutzmaßnahme an, langfristig

Im *M-Trends 2018 Report* von Fireye wird beschrieben, dass die globale durchschnittliche Verweildauer von einem Angreifer in einem Netzwerk im Jahr 2017 101 Tage betragen hat. Die Verweildauer sagt aus, wie viele Tage zwischen dem ersten Anzeichen einer Angreifer-Aktivität bis zur Aufdeckung des Angriffs vergangen sind.[43]

2.6 Schutzvorkehrungen

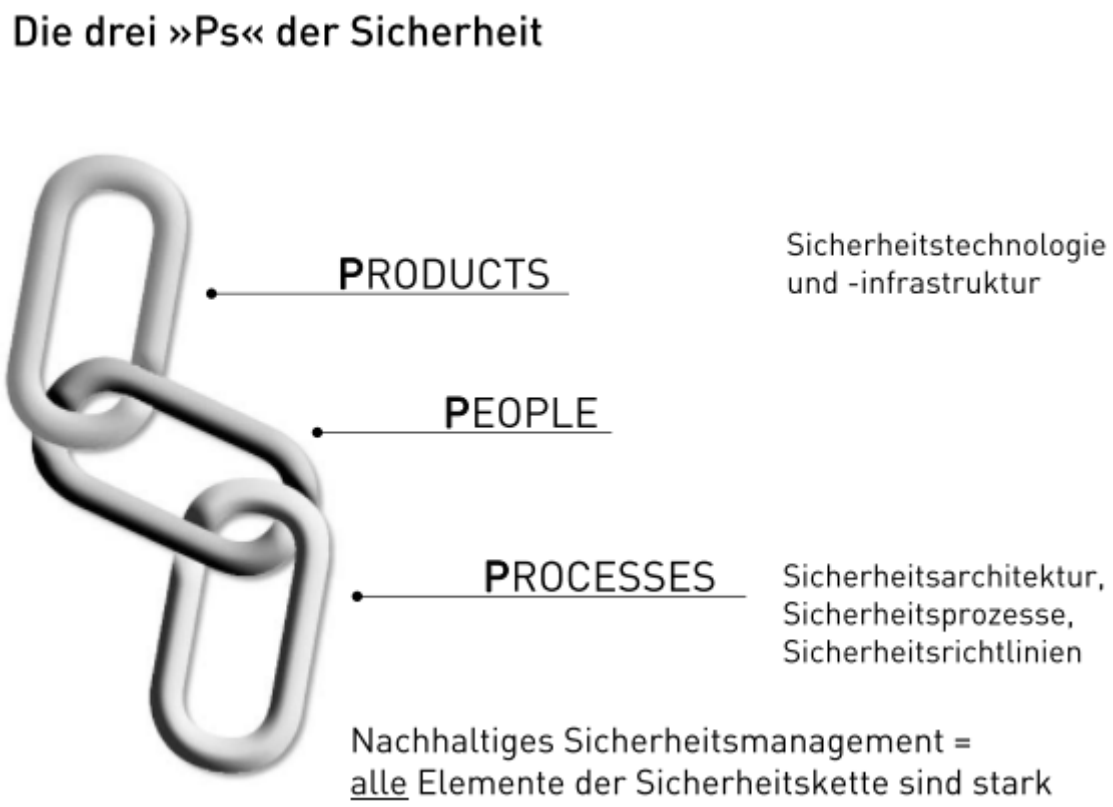
Unternehmen setzen Schutzvorkehrungen ein, um sich vor Angreifern bzw. Angriffen zu schützen. In diesem Kapitel wird erläutert, welche Faktoren wichtig sind, um ein

[39] Vgl. *Luber, S./Schmitz, P.*, Was ist ein Exploit?, 2017.
[40] Vgl. *Hellmann, R.*, IT-Sicherheit, 2018, S. 119.
[41] Vgl. *BSI*, Die Lage der IT-Sicherheit in Deutschland 2018, 2018., S. 23, 96.
[42] Vgl *Decker, B.* de/*Zúquete, A.*, Communications and multimedia security, 2014, S. 65.
[43] *FireEye*, M-Trends 2018.

nachhaltiges Sicherheitsmanagement zu erreichen und welche Ansätze in der Praxis eingesetzt werden.

In der Informationssicherheit wird der Faktor Mensch als der Erfolgsfaktor gesehen. Den Menschen zu verstehen, zu erreichen, zu überzeugen und zu verändern, ist dabei die große Aufgabe des IT-Security-Awareness, welcher dem deutschen Begriff Sicherheitsbewusstsein entspricht. In der Sicherheitskette aus Produkten (Sicherheitstechnologie und -infrastruktur), Prozessen (Sicherheitsarchitektur, Sicherheitsprozesse, Sicherheitsrichtlinien) und Menschen (engl. 3 P = Product, Process, People) ist der Mensch das Bindeglied. Ein nachhaltiges Sicherheitsmanagement kann nur erreicht werden, wenn alle Elemente der Sicherheitskette stark und aufeinander abgestimmt sind (siehe Abbildung 5: Die drei "Ps" der Sicherheit).[44]

Abbildung 5: Die drei "Ps" der Sicherheit[45]



Defense in Depth (auch bekannt als Castle / Multi-Layer-Approach) ist eine Sicherheitsarchitektur, die in verschiedene Schichten (Verteidigungsschichten) und Ebenen unterteilt ist. Ursprünglich kommt diese Verteidigungsstrategie aus dem Mittelalter und wurde später auf Informationssicherheit übertragen.[46] In diesem Prinzip wird

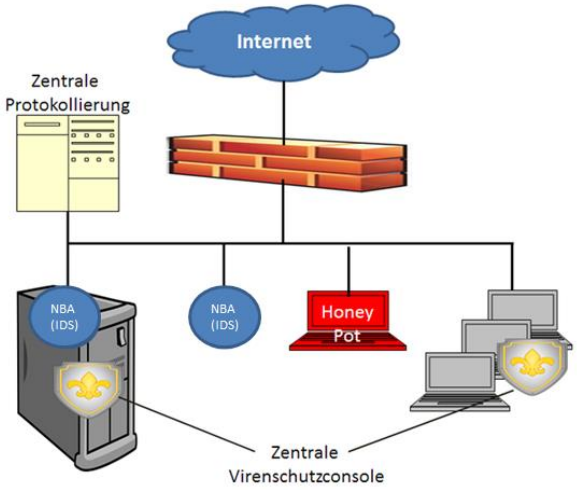
> jede Schicht [.] mit verschiedenen Sicherheitsmaßnahmen versehen. Überwindet ein Angreifer eine Schicht, z. B. eine Firewall, dann steht er schon vor der nächsten Sicherheitsmaßnahme. Als Analogie

[44] Vgl. *Helisch, M./Pokoyski, D./Beyer, M.*, Security Awareness, 2009, S. 12-13.
[45] Vgl. *Helisch, M./Pokoyski, D./Beyer, M.*, Security Awareness, 2009, S. 13.
[46] Vgl. *Small, P.*, Defense in Depth: AnImpractical Strategy for a Cyber World, 2018.

dafür wird gerne das Bild der Burg hergenommen. Eine standhafte Burg besteht aus mehr als nur der Burgmauer allein. Sie besitzt einen Burggraben mit Zugbrücke, diverse Innenmauern und Verteidigungstürme. Jede Maßnahme dient einem anderen Zweck – der Burggraben verlangsamt den Angreifer, die Türme bieten Platz für Bogenschützen und die Unterteilung durch Innenmauern vermindert die Ausbreitung von Feuern […]. Nur im Zusammenwirken aller Maßnahmen wird die Burg zu einer standhaften Festung.[47]

In der folgenden Abbildung wird das Unternehmen vor unerwünschten Verbindungen aus dem Internet mit einer Firewall geschützt, zusätzlich gibt es eine zentrale Protokollierung zur Auswertung von Log-Daten. Weitere Sicherheitsmaßnahmen sind ein Intrusion Detection System zur Erkennung von Angriffen und ein Honey Pot, um Angreifer auf eine falsche Fährte zu locken und zu entlarven. Zudem sind die Clients durch einen Virenschutz geschützt, der über eine zentrale Virenschutzkonsole überwacht wird. Dies soll als Beispiel verdeutlichen, wie ein Defense in Depth in einem Unternehmen umgesetzt sein kann.

Abbildung 6: Defense in Depth[48]



Die Verteidigungslinien einer Sicherheitsinfrastruktur können in die Maßnahmen der Prävention, Detektion und Reaktion aufgeteilt werden. Präventive Maßnahmen sollen IT-Sicherheitsvorfällen vorbeugen, d. h. dem Eintritt unerwünschter Folgen entgegenwirken, in dem dieser verhindert wird. Eine solche Maßnahme ist beispielsweise, wenn nur freigegebene Programme auf einer Whitelist ausgeführt werden dürfen. Bei der Detektion geht es darum, einen eingetretenen Vorfall zu erkennen. Ein Beispiel hierfür ist eine Virenschutzsoftware, die erkennt, sobald ein Virus ausgeführt wird. Das Ziel von reaktiven Maßnahmen ist es, die Auswirkungen von einem IT-Sicherheitsvorfall zu begrenzen und einen sicheren Zustand der betroffenen Systeme wiederherzustellen. So könnte beispielsweise der Netzwerkzugang von einer betroffenen Anwendung automatisch unterbunden werden, bis der Vorfall untersucht und ggf. die notwendigen Maßnahmen, wie das Einspielen von Sicherheitspatches, vorgenommen wurde.

[47] Vgl. *Weidele, M.*, Warum Ihre nächste Security-Investition nach Defense-In-Depth erfolgen sollte, 2018.
[48] Vgl. *Wege, O.*, Datei:Defense-in-Depth1.png, 2016.

Das Spektrum der Maßnahmen der Prävention, Detektion und Reaktion ist breit und kann sowohl technische als auch organisatorische Maßnahmen umfassen. Auch rechtliche Maßnahmen, wie die Einführung von Gesetzen, können die Anzahl an IT-Sicherheitsvorfällen für Unternehmen verringern.[49]

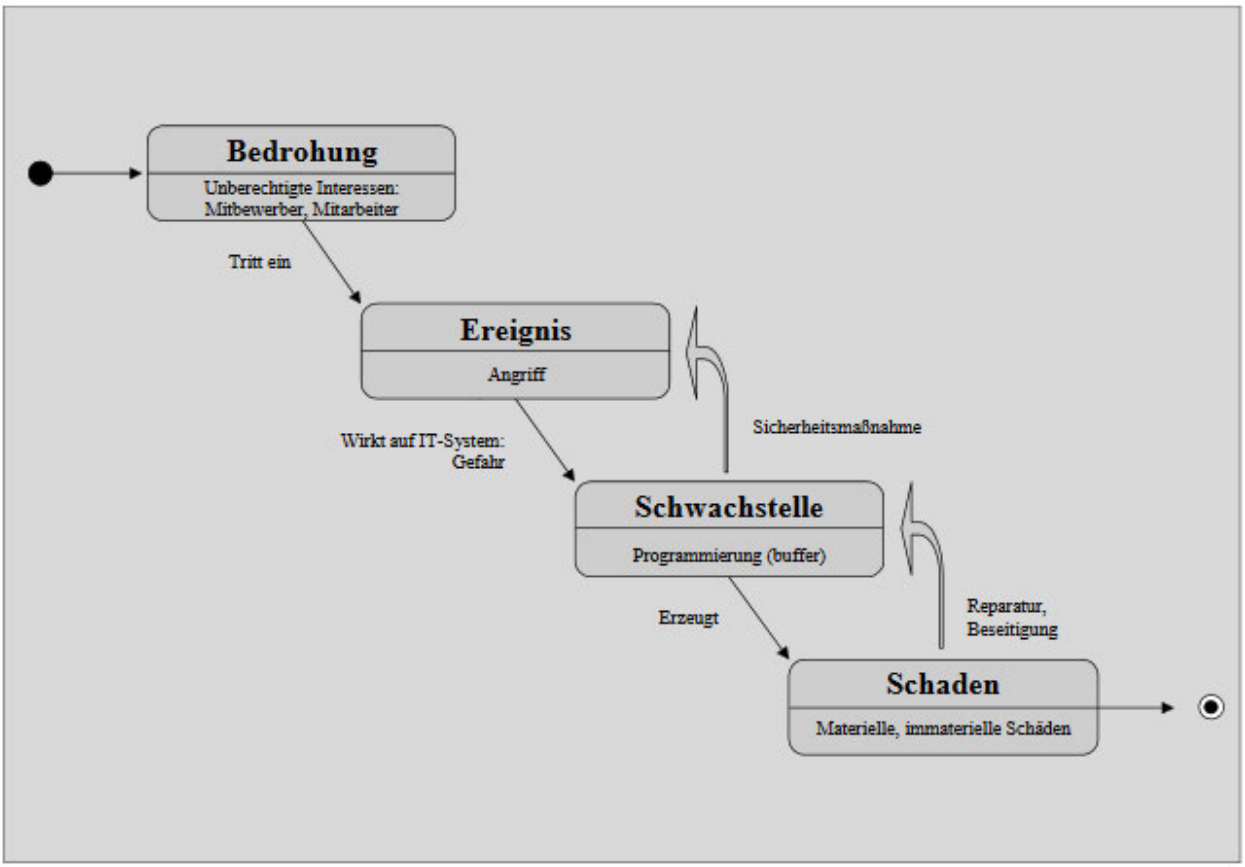
2.7 Angriffs- / Schadensmodell

Das in diesem Kapitel erläuterte Angriffs- und Schadensmodell soll ein vereinfachtes Abbild der Wirklichkeit darstellen, um die Zusammenhänge zwischen den beschriebenen theoretischen Grundlagen zu verstehen.

Eine Bedrohung für ein Unternehmen kann das unberechtigte Interesse von Mitbewerbern oder Mitarbeitern sein. Das tatsächliche Eintreten einer Bedrohung, wie ein Angriff auf das Unternehmen, ist ein Ereignis. Das Ereignis birgt die Gefahr, dass es auf ein IT-System einwirkt. Eine Schwachstelle kann durch einen Fehler in der Programmierung z. B. durch einen zu klein reservierten Speicherbereich für eine zu große Datenmenge entstehen. Wenn die Schwachstelle ausgenutzt wird, kann ein Schaden an materiellen oder immateriellen Gütern entstehen. Damit nicht erneut ein Schaden eintreten kann, muss eine Schwachstelle behoben werden. Dies kann z. B. das Installieren eines Patches, die Änderung des Programmiercodes oder eine Konfigurationsanpassung sein. Das Modell wurde in der Abbildung 7: Schadensmodell visualisiert.

[49] Vgl. *Hoppe, T.*, Prävention, Detektion und Reaktion gegen drei Ausprägungsformen automotiver Malware, 2014, S. 13-14.

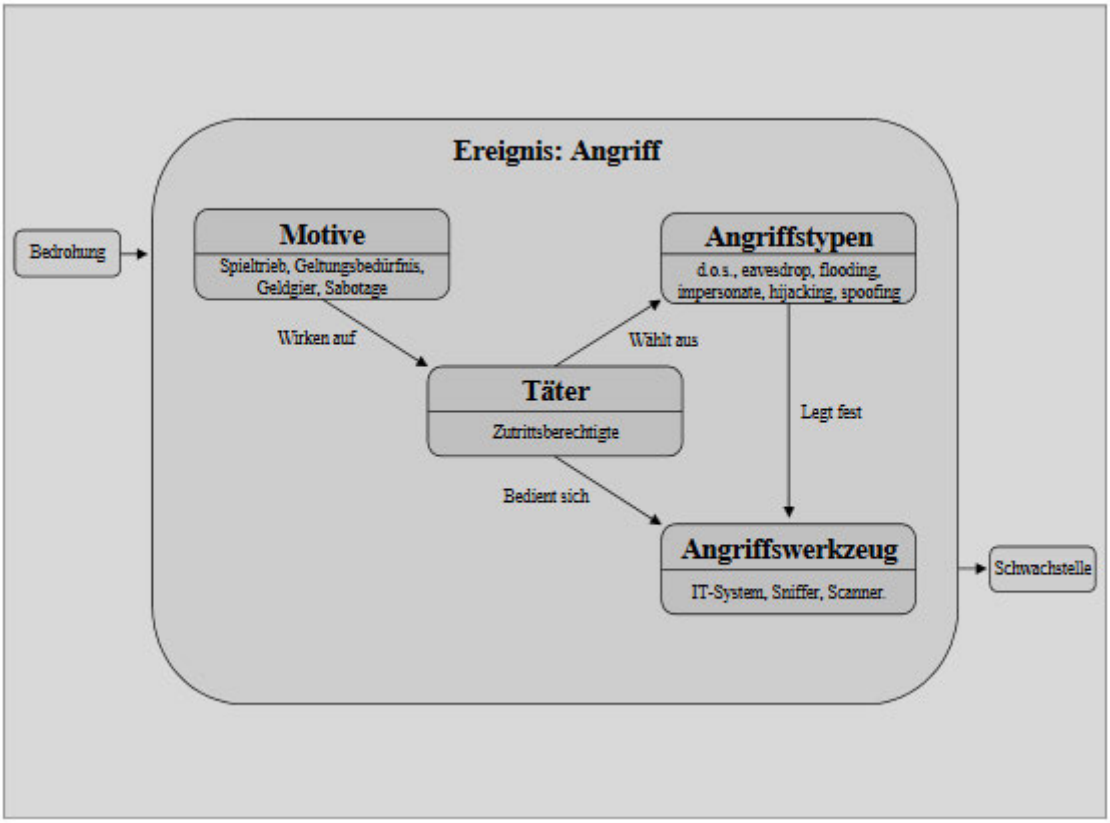
Abbildung 7: Schadensmodell[50]



Für einen tatsächlichen Angriff kann ein Täter unterschiedliche Motive, wie bspw. den Spieltrieb, Geltungsbedürfnis, Geldgier und Sabotage haben. Der Täter kann ein interner Mitarbeiter mit Zutrittsberechtigung oder eine Person ohne Zutrittsberechtigung sein. Ein Täter bedient sich an Angriffswerkzeugen, wie einem IT-System, einem Netzwerksniffer oder Scanner und wählt Angriffstypen aus. Je nach Angriffstypen wird das Angriffswerkzeug festgelegt und eine Schwachstelle ausgenutzt. Das Angriffsmodell wurde in der Abbildung 8: Angriffsmodell visualisiert.

[50] *Pohl, H.*, Taxonomie und Modellbildung in der Informationssicherheit, 2004, S. 682.

Abbildung 8: Angriffsmodell[51]



2.8 Audit

Die Durchführung von Audits (dt. Überprüfung) ist eine traditionsreiche und anerkannte Methode, um einen Istzustand mit einem Sollzustand abzugleichen. Ursprünglich wurde diese Methode eingesetzt, um die Geschäftsbücher zu prüfen. Die Prüfung erfolgte mündlich durch öffentlichen Vortrag. So erklärt sich die Herkunft aus dem lateinischen auditius.[52]

Bei Audits im Zusammenhang mit IT-Sicherheit wird die Konformität von einem Unternehmen zu einem Standard wie der ISO/IEC 27001 geprüft. Anhand des ISO/IEC 27001-Standard soll die Vorgehensweise bei einem Audit zur Konformitätsprüfung analysiert werden.

2.8.1 ISO/IEC 27001 Audit

Bei einem Audit bezüglich der ISO/IEC 27001 geht es um die Feststellung des aktuellen Zustands des Informationssicherheitsmanagementsystems (ISMS) und den Vergleich mit dem Sollzustand der Anforderungen aus dem Standard. In folgender Tabelle werden die relevanten Standards zur Durchführung eines ISO/IEC 27001-Audits aufgelistet.

[51] *Pohl, H.*, Taxonomie und Modellbildung in der Informationssicherheit, 2004, S. 683.
[52] Vgl. *Kersten, H.* u. a., IT-Sicherheitsmanagement nach der neuen ISO 27001, 2016, S. 75.

Abbildung 9: Relevante Standards für ISO 27001 Audits

Standard	Titel	Kurzbeschreibung
ISO/IEC 27001	IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen	In diesem Standard werden die Anforderungen für die Einrichtung, Implementierung, Wartung und der laufenden Verbesserung eines ISMS festgelegt.
ISO/IEC 27006	Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems	Diese Norm legt Anforderungen fest und gibt Leitlinien für Stellen, die die Audits und die Zertifizierung eines ISMS durchführen.
ISO/IEC 27007	Information technology - Security techniques - Guidelines for information security management systems auditing	Dieser Standard enthält Hinweise zur Verwaltung eines ISMS Auditprograms, zur Durchführung von Audits und zur Kompetenz der ISMS-Auditoren, zusätzlich zur ISO 19011.
ISO/IEC TS 27008	Information technology - Security techniques - Guidance for auditors on information security management systems controls	Der Standard bietet eine Leitlinie zur Überprüfung und Bewertung von Informationssicherheitskontrollen, die über ein nach ISO/IEC 27001 spezifiziertes Informationssicherheitsmanagementsystem verwaltet werden.
ISO 19011	Leitfaden zur Auditierung von Managementsystemen	Eine Anleitung zum Auditieren von Managementsystemen, einschließlich Auditprinzipien, der Steuerung eines Auditprogramms und der Durchführung von Audits von Managementsystemen, sowie zur Beurteilung der Kompetenz derer, die in den Auditprozess einbezogen sind.

Beim Audit wird der Ist-Zustand zum Zeitpunkt der Durchführung geprüft. Ein Audit ist eine Breitenprüfung in der nicht alle Aspekte aufgrund der zeitlichen Begrenzung vollständig geprüft werden können, d. h. das Auditergebnis ist beschränkt auf eine qualifizierte Stichprobe. Erst nach mehreren Audits ergibt sich dann ein vollständiges Bild für einen Auditor. Der grundsätzliche Ablauf in einem Audit wird in folgender Tabelle beschrieben.[53]

Tabelle 7: Ablauf Audit

Ablauf	Kurzbeschreibung
Planung	Durchführung der Auditplanung (Auditgegenstand, Ziel und Ablauf des Audits, erforderliche Personen) zwischen Auditor und den Beteiligten wird abgestimmt. Der Auditor bereitet das Audit z. B. ein Fragenkatalog oder Checklisten vor.

[53] Vgl. *Kersten, H.* u. a., IT-Sicherheitsmanagement nach der neuen ISO 27001, 2016, S. 75 ff.

Ablauf	Kurzbeschreibung
Inhalte	Das Unternehmen stellt den Ist-Stand bzw. die Änderungen gegenüber dem letzten Audit vor und der Auditor stellt Fragen, dokumentiert und äußert ggf. Korrekturwünsche.
Prüfung	In dieser Phase wird die Übereinstimmung von der Dokumentation zur Realität geprüft. Durch Interviews und Ortsbegehungen werden objektive Nachweise gesammelt und Defizite aufgedeckt.
Ergebnisdarstellung	Am Ende des Audits werden die Prüfergebnisse zusammengefasst und präsentiert, sowie die weitere Vorgehensweise zur Behebung von Feststellungen besprochen.

Bei einem Audit geht es darum Konformität zu prüfen bzw. Nicht-Konformität festzustellen. Aus diesem Grund werden Konfirmitätsnachweise gesammelt (siehe Tabelle 8: Arten von Audit-Nachweisen). Die Tabelle wurde auf Basis von Schulungsunterlagen zum ISMS ISO/IEC 27001 Auditor erstellt.

Tabelle 8: Arten von Audit-Nachweisen

Art	Beschreibung	Beispiel
Physisch	Ein physischer Gegenstand kann gezählt, geprüft, beobachtet oder inspiziert werden.	Das Vorhandensein von Brandschutzvorrichtungen prüfen
Mathematisch	Der mathematische Beweis besteht aus mathematischen Berechnungen, die vom Auditor durchgeführt werden.	Berechnung der Anzahl der Schulungsstunden, die im Zusammenhang mit dem ISMS durchgeführt werden Anschließend kann das Ergebnis mit dem Ziel verglichen werden.
Bestätigend	Beweise, die von externen Dritten stammen. Die Zuverlässigkeit dieser Art von Beweismitteln hängt von der Zuverlässigkeit ab, die die auditierte Organisation dem Dritten, der die Beweise liefert, verleihen kann.	Schreiben eines Anwalts, das die Gesetze, denen ein Unternehmen unterliegt, bestätigt
Technisch	Analyseergebnisse von technischen Tests oder Beobachtungen, die an einem Informationssystem durchgeführt wurden.	Ergebnisbericht eines Penetrationstest.
Analytisch	Analytische Beweise bestehen aus den Ergebnissen aus dem Verhältnis zwischen der aufgezeichneten Analyse und den Erwartungen des Auditors. Alle mit den statistischen Methoden	Analyse von Tickets für Sicherheitsvorfälle

Art	Beschreibung	Beispiel
	gesammelten Beweise sind analytisch. Analytische Beweise bestehen in der Analyse von Daten und deren Variationen, um deren Tendenzen und mögliche Abweichungen zu erkennen.	
Dokumentarisch	dokumentierte Beweise	Prüfung einer Leitlinie oder Richtlinie
Verbal	Verbale Beweise sind die Beweise, die bei Interaktionen zwischen dem Auditor und dem Personal der geprüften Stelle gesammelt werden.	Diskussionen, die während des Audits geführt wurden

Um die Nachweise zu sammeln, werden die folgenden Testmethoden angewandt:[54]

- Beobachtung
- Befragung
- Analyse
- Bestätigung
- Untersuchung

Generell geht es um die Überprüfung der IT-Infrastruktur hinsichtlich Ordnungsmäßigkeit, Effizienz und Effektivität. Das Audit ist keine technische Prüfung und nicht darauf fokussiert, angreifbare Schwachstellen aufzudecken. Die Prüfung erfolgt anhand von Fragenkatalogen und Checklisten.[55] Die ISO/IEC 27001 Audits lassen sich in unterschiedliche Typen, die in folgender Tabelle beschrieben sind, einteilen.

Tabelle 9: Audit-Typen[56]

Audit-Typ	Beschreibung
Preaudit / Readiness Audit / Stage-1-Audit	Wird im Rahmen der Einführungsphase eines ISMS durchgeführt, um zu prüfen, ob alle wesentlich identifizierbaren Prozessse, Regeln und Maßnahmen des ISMS umgesetzt sind. Ziel ist es, herauszustellen, ob das ISMS bereits den Reifegrad hat, um ein Zertifizierungsaudit durchzuführen.
Internes Audit / Stage-2-Audit	Der Standard verlangt die Planung, Umsetzung und regelmäßige Durchführung von internen Audits. Interne Audits werden von unabhängigen Auditoren durchgeführt. Hier kommen in der Regel interne Auditoren zum Zuge (auch wenn eine externe Beauftragung möglich ist).
Zertifizierungsaudit	Wenn das ISMS eingeführt ist und die Zertifizierung angestrebt wird, wird das Zertifizierungsaudit durchgeführt. Von der

[54] Vgl. *Sowa, A./Duscha, P./Schreiber, S.*, IT-Revision, IT-Audit und IT-Compliance, 2019.
[55] Vgl. *BSI*, Studie Durchführungskonzept für Penetrationstests, S. 10.
[56] Vgl. *Kersten, H.* u. a., IT-Sicherheitsmanagement nach der neuen ISO 27001, 2016, S. 33, 81.

Audit-Typ	Beschreibung
	ausgesuchten Zertizierungsstelle wird ein externer Auditor oder ein externes Auditorenteam beauftragt.
Überwachungsaudit	Bei einem Überwachungsaudit wird eine bestehende Zertifizierung überwacht. Es findet zwischen dem Gültigkeitsbeginn und -ende des Zertifikats statt. In der Regel beträgt der zeitliche Abstand 12 Monate und wird von externer Seite durchgeführt.
Re-Zertifizerungsaudit	Damit eine Zertifizierung kontinuierlich gewährleistet ist, muss vor Ablauf des drei Jahre gültigen Zertifikats ein Re-Zertifizierungsaudit durchgeführt werden. Das Audit wird von externen Auditoren durchgeführt.
Special Audits	Bei Änderungen des Anwendungsbereiches, der Organisationsstruktur oder bei Prüfung von Hinweisen oder Beschwerden, kann ein Special Audit durchgeführt werden.

2.8.2 Cyber-Sicherheits-Check

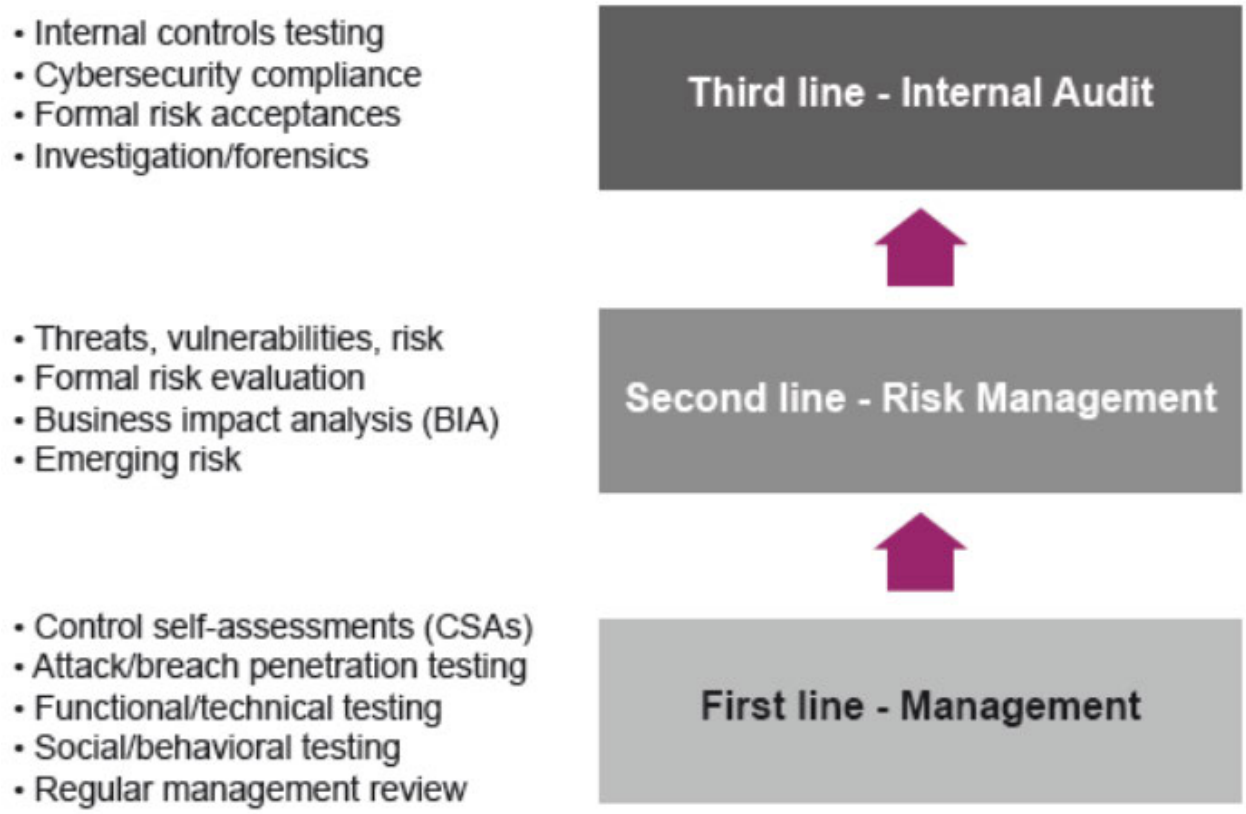
In einem Penetrationstest wird selektiv ein Testgegenstand auf Schwachstellen geprüft. Er gibt keine Aussage über den allgemeinen Zustand der Cyber-Sicherheit. Auch die ISO/IEC 27001 oder der BSI-Grundschutz stellt kleine und mittelständische Unternehmen häufig vor eine große Herausforderung und ein Audit scheitert bereits an fehlenden formalen Dokumenten.[57] Aus diesem Grund hat das BSI im Jahr 2015 im Rahmen der Allianz für Cyber-Sicherheit in Kooperation mit ISACA Germany Chapter e.V. das Projekt „Cyber-Sicherheits-Check“ (CSC) initiiert.

Der CSC richtet sich vor allem an kleine und mittlere Unternehmen und soll einen niederschwelligen Ansatz zur Überprüfung des Stands der Cyber-Sicherheit bieten. Die Grundlage des CSC sind die vom BSI veröffentlichten Basismaßnahmen der Cyber-Sicherheit, welche sich in den Maßnahmenzielen des Cyber-Sicherheits-Checks wiederfinden. Die Prüfung können Unternehmen anhand des „Leitfaden Cyber-Sicherheits-Check“ selbst durchführen oder sich von einen zertifizierten „Cyber-Security-Practitioner“ unterstützen lassen.[58] Der Leitfaden umfasst die Überprüfung der Sicherheitsmaßnahmen, die eine Institution und Einzelperson davor bewahren soll, Opfer eines Cyber-Angriffs zu werden. Er ist so konzipiert, dass die APT-Angriffe grundsätzlich erschwert und die Fähigkeit zur Entdeckung eines Angriffs und zur adäquaten Reaktion gestärkt werden. Das Risiko, einem APT-basierten Cyber-Angriff zum Opfer zu fallen, soll durch regelmäßige Durchführung des CSC minimiert werden.

Im CSC wird von drei Verteidigungslinien gesprochen (siehe Abbildung 10: Drei Verteidigungslinien).

[57] Vgl. *Bartsch, M./Frey, S.*, Cybersecurity Best Practices, 2018, S. 464.
[58] Vgl. *BSI*, Cyber-Sicherheit, 2019.

Abbildung 10: Drei Verteidigungslinien[59]



Zur ersten Linie gehört das Verständnis der Leitung bzw. des Managements zur Cyber-Sicherheit. Es geht darum den Schutzbedarf und Abhängigkeiten von Geschäftsprozessen festzulegen. Das Risikomanagement ist die zweite Linie. Dort kommt es zu einer Analyse, in wie weit sich Cyber-Sicherheitsrisiken auf die Institution und deren Prozesse auswirken. Das Risikomanagement prüft als erste unabhängige Instanz die Entscheidungen des Managements und bewertet diese, ohne die Beschlüsse rückgängig zu machen, da die finale Entscheidung über die Umsetzung von Sicherheitsmaßnahmen bei dem Management verbleibt. Erst in der dritten Linie kommt der CSC zum Einsatz. Hiermit wird das vorhandene Sicherheitsniveau durch eine unabhängige und objektive Beurteilung geprüft. Indem der Beurteiler systematisch und zielgerichtet die Institution bewertet, unterstützt er bei der Erreichung der Ziele und fördert die Optimierung der Sicherheitsmaßnahmen. Bei einem CSC soll der laufende Betrieb der Institution nicht wesentlich gestört werden und der Beurteiler greift niemals selbst aktiv in ein System ein und erteilt auch keine Handlungsanweisungen zu Änderungen an IT-Systemen, Infrastrukturen, Dokumenten oder organisatorischen Abläufen.

Bei der Durchführung eines CSC ist die gesamte Institution einschließlich ihrer Anbindungen an das Internet, über andere Organisationseinheiten und an Netze, Gegenstand der Prüfung. Physische Aspekte wie der Bandschutz und Einbruchsschutz sind nicht relevant für die Prüfung. Um ein CSC durchzuführen müssen weder obligatorische Dokumente zum

[59] *BSI/ISACA*, Leitfaden Cyber-Sicherheits-Check, 2014, S. 18.

Sicherheitsprozess existieren, noch muss ein definierter Umsetzungsstatus bestimmter Sicherheitsmaßnahmen erreicht sein.[60] In der folgenden Tabelle wird die Vorgehensweise schrittweise erläutert:

Abbildung 11: Schritte bei der Durchführung des CSC[61]

Schritt		Beschreibung
1	**Auftragserteilung**	Im ersten Schritt gibt die Leitung/ das Management einen Auftrag zur Durchführung des CSC.
2	**Bestimmung der Cyber-Sicherheits-Exposition**	Der zu erwartende Zeitaufwand, die Beurteilungstiefe und die Wahl der Stichproben werden in der Cyber-Sicherheits-Exposition (CSE) bestimmt. Als Anhaltspunkte zur Bestimmung dienen Kurzinterviews oder vorhandene Erfahrungswerte. Das CSE wird im Bericht dokumentiert.
3	**Dokumentensichtung**	In der Dokumentensichtung geht es darum, einen Überblick über die Aufgaben, die Organisation und die IT-Infrastrukturen der Institution zu gewinnen. Sie besteht nur aus einer groben Sichtung der zur Verfügung gestellten Dokumente. Zu den Dokumenten zählen bspw. ein IT-Rahmenkonzept, IT-Sicherheitsleitlinie/ -konzept oder ein Netzplan. Wenn keine Dokumente vorhanden sind, wird der Überblick durch Interviews verschafft. Auf Grundlage der Erkenntnisse werden die Stichproben und Schwerpunkte der Beurteilung bestimmt.
4	**Vorbereitung der Vor-Ort-Beurteilung**	Als Vorbereitung wird ein Ablaufplan mit Einbeziehung der CSE erstellt, der darstellt, welche Inhalte wann beurteilt werden und welche Ansprechpartner hierzu erforderlich sind.
5	**Vor-Ort-Beurteilung**	Die Vor-Ort-Beurteilung startet mit einem Eröffnungsgespräch indem die Vorgehensweise, die Zielrichtung und die organisatorischen Punkte geklärt werden. Anschließend werden Interviews geführt, IT-Systeme in Augenschein genommen und evtl. weitere Dokumente gesichtet. Die Stichproben (z. B. Dokumente, IT-Systeme) und die Sachverhalte werden im Laufe des Tages vom Beurteiler ausreichend dokumentiert, um diese Informationen für die Erstellung des Berichts verwenden zu können. Die Vor-Ort-Beurteilung endet mit einem Abschlussgespräch, an dem auch die Leitungsebene teilnehmen sollte. Hier werden erste allgemeine Einschätzungen über das Niveau der Cyber-Sicherheit und eventuelle schwerwiegende Sicherheitsmängel, die die Institution stark gefährden und zeitnah behandelt werden sollen, präsentiert.
6	**Nachbereitung / Berichterstellung**	Der Abschluss des CSC ist ein Beurteilungsbericht mit einem Überblick zur Cyber-Sicherheit in der Institution, dem CSE

[60] Vgl. *BSI/ISACA*, Leitfaden Cyber-Sicherheits-Check, 2014, S. 12-13, 18-19.
[61] Vgl. *BSI/ISACA*, Leitfaden Cyber-Sicherheits-Check, 2014, S. 23-26.

Schritt		Beschreibung
		und einer Liste der festgestellten Mängel. Zur Behandlung der Mängel werden allgemeine Empfehlungen aufgezeigt, damit ein Unternehmen beurteilen kann, in welchen Bereichen vermehrt Aktivitäten erforderlich sind, um das Cyber-Sicherheits-Niveau zu erhöhen.

Die Beurteilungsmethoden im CSC entsprechen denen eines Audits. Die Methoden sind vom konkreten Sachverhalt abhängig und werden durch den Beurteiler festgelegt. Es können auch mehrere Methoden kombiniert werden, allerdings muss der Beurteiler den Grundsatz der Verhältnismäßigkeit einhalten. Die gefundenen Sicherheitsmängel werden nach Kritikalität in kein Sicherheitsmangel, Sicherheitsempfehlung, Sicherheitsmangel und schwerwiegender Sicherheitsmangel eingeordnet. Kein Mangel bedeutet, dass es keine Hinweise gibt. Eine Empfehlung wird geschrieben, wenn die Sicherheit erhöht werden kann, es Verbesserungsvorschläge für die Umsetzung von Maßnahmen, ergänzende Maßnahmen, die sich bewährt haben oder Kommentare hinsichtlich der Angemessenheit von Maßnahmen aufgeführt werden müssen. Bei einem Sicherheitsmangel liegt eine Sicherheitslücke vor. Dies sollte mittelfristig behoben werden, da die Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen beeinträchtigt werden kann. Der schwerwiegende Sicherheitsmangel im CSC ist eine Sicherheitslücke, die umgehend geschlossen werden sollte, da die Vertraulichkeit, die Integrität und/ oder die Verfügbarkeit der Informationen stark gefährdet sind und erheblicher Schaden zu erwarten ist. Die Dokumentation sollte im Abschlussbericht so dokumentiert sein, dass sie für einen sachkundigen Dritten nachvollziehbar ist.[62]

Im Rahmen der Masterarbeit wurde ein CSC-erfahrener Cyber-Security Pracitioner interviewt, (siehe Anlage 1 Interview Cyber Security Pracitioner), um seine Erfahrung in die Arbeit einfließen lassen zu können.

2.8.3 Fazit

Generell geht es bei einem Audit darum, den Ist-Zustand mit einem Soll-Zustand zu vergleichen. Bei einem ISO/IEC 27001 Audit wird die Konformität zum Standard geprüft. Beim CSC werden die entwickelten Maßnahmenziele von ISACA und dem BSI begutachtet und der Stand bezüglich Cyber-Sicherheit festgestellt. Dabei werden mögliche Sicherheitsmängel und Verbesserungspotenziale aufgedeckt. Bei beiden Verfahren werden auf Grundlage einer qualifizierten Stichprobe Audit-Nachweise gesammelt. Die Prüfung erfolgt durch Beobachtung, Dokumentenprüfung, Interview, Analyse und technische Prüfung. Bei der technischen Prüfung darf der Auditor nicht selbst Hand anlegen, sondern sich nur Systeme zeigen lassen oder Dokumente prüfen. Ein Audit ist abhängig vom verwendeten Standard. Der CSC richtet sich vor allem an die Unternehmen, die noch wenig bezüglich Informationssicherheit dokumentiert und kein ISMS implementiert haben.

[62]Vgl. *BSI/ISACA*, Leitfaden Cyber-Sicherheits-Check, 2014, S. 28-29.

2.9 Penetrationstest

2.9.1 Bundesamt für Sicherheit in der Informationstechnik

Ein Penetrationstest ist ein geeignetes Verfahren, um die aktuelle Sicherheit eines IT-Netzes, eines einzelnen IT-Systems oder einer (Web)-Anwendung festzustellen. Mit dessen Hilfe können die Erfolgsaussichten eines vorsätzlichen Angriffs eingeschätzt und die Wirksamkeit vorhandener Sicherheitsmaßnahmen geprüft sowie weitere notwendige Maßnahmen abgeleitet werden.[63] Das Aufspüren von Sicherheitslücken erfordert eine gewisse Erfahrung und kontinuierliche Übung, da ständig neue Sicherheitslücken hinzukommen und einbezogen werden müssen. Dies können IT-Mitarbeiter in der Regel nicht leisten. Aus diesem Grund werden Spezialunternehmen mit einem Penetrationstest beauftragt. Die Art und der Umfang sind bei einem Test begrenzt. Dies kann dazu führen, dass Lücken unentdeckt bleiben. Die wichtigen Sicherheitslücken sollten aber nach einem Test behoben werden, damit Angreifer es schwer haben, in ein Unternehmen einzudringen und die Gefahr sinkt, dass ein erfolgreicher Angriff durchgeführt wird.[64]

In der Studie vom BSI *„Durchführungskonzept für Penetrationstest"* wurde 2003 folgende Definition für Penetrationstests veröffentlicht:

> Im technischen Sprachgebrauch versteht man unter einem Penetrationstest den kontrollierten Versuch, von „außen" in ein bestimmtes Computersystem bzw. -netzwerk einzudringen, um Schwachstellen zu identifizieren. Dazu werden die gleichen bzw. ähnlichen Techniken eingesetzt, die auch bei einem realen Angriff verwendet werden. Die hierbei identifizierten Schwachstellen können dann durch entsprechende Maßnahmen behoben werden, bevor diese von unautorisierten Dritten genutzt werden können.[65]

Im Jahr 2016 wurde vom BSI der *„Praxis-Leitfaden für IS-Penetrationstests"* veröffentlicht. Ein Informationssicherheit (IS) Penetrationstest wird wie folgt beschrieben:

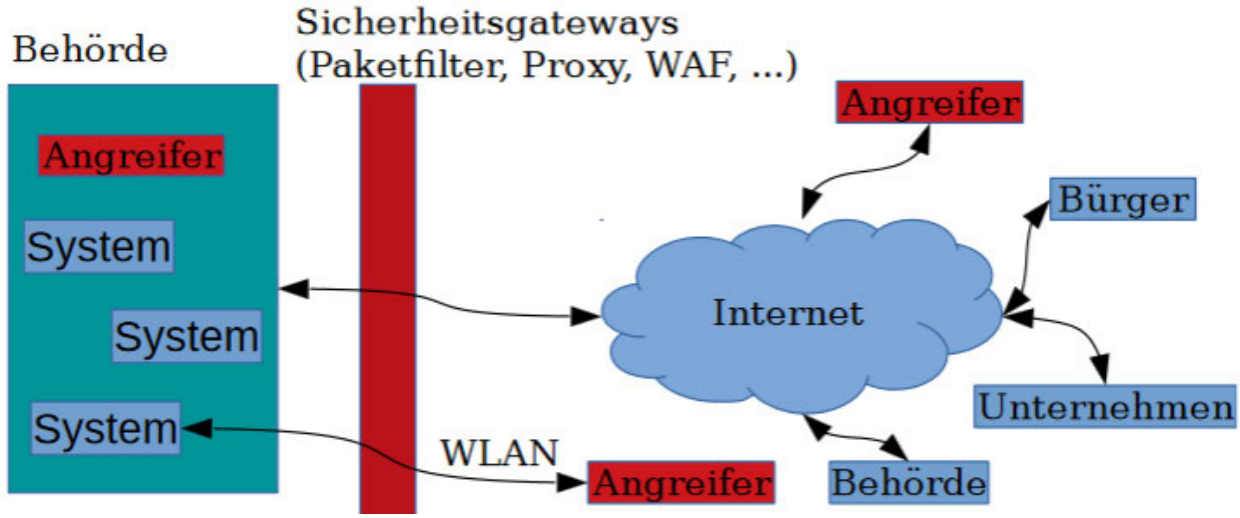
> Ein IS-Penetrationstest ist ein erprobtes und geeignetes Vorgehen, um das Angriffspotenzial auf ein IT-Netz, ein einzelnes IT-System oder eine (Web-) Anwendung festzustellen. Hierzu werden die Erfolgsaussichten eines vorsätzlichen Angriffs auf einen Informationsverbund oder ein einzelnes IT-System eingeschätzt und daraus notwendige ergänzende Sicherheitsmaßnahmen abgeleitet, beziehungsweise die Wirksamkeit von bereits umgesetzten Sicherheitsmaßnahmen überprüft. Im Detail werden dabei die installierten IT-Anwendungen (Webanwendung, Mailserver, etc.) beziehungsweise die zugrunde liegenden Trägersysteme (Betriebssystem, Datenbank, etc.) überprüft. Typische Ansatzpunkte für einen IS-Penetrationstest sind:
>
> - Netzkoppelelemente (Router, Switches, Gateways)
> - Sicherheitsgateways (Firewall, Paketfilter, Intrusion Detection System, Virenscanner, Loadbalancer etc.)
> - Server (Datenbankserver, Webserver, Fileserver, Speichersysteme, etc.)
> - Telekommunikationsanlagen

[63] Vgl. *BSI*, IS-Penetrationstest und IS-Webcheck..
[64] Vgl. *Hellmann, R.*, IT-Sicherheit, 2018, S. 177.
[65] *BSI*, Studie Durchführungskonzept für Penetrationstests, S. 4.

- Webanwendungen (Internetauftritt, Vorgangsbearbeitung, Webshop)
- Clients
- Drahtlose Netze (WLAN, Bluetooth)
- Infrastruktureinrichtungen (Zutrittskontrollmechanismen, Gebäudesteuerung)[66]

Am 16. Juli 2018 wurde das Dokument *„IS-Webcheck – Sicherheits-Check für Webauftritte durch das BSI“* veröffentlicht. Kurz darauf am 01. August 2018 hat das BSI ein Dokument mit der Bezeichnung *„IS-Penetrationstest – Penetrationstest von IT-Systemen durch das BSI“* hochgeladen.[67] In diesen Dokumenten wird der IS-Webcheck und IS-Penetrationstest beschrieben, der vom BSI für Bundesbehörden oder Betreiber kritischer Infrastrukturen angeboten wird. Bei einem IS-Webcheck wird ein Webauftritt oder deren Teilbereiche mit automatischen Verfahren auf Schwachstellen getestet.[68] Im IS-Penetrationstest werden IT-Systeme auf vorhandene Schwachstellen untersucht. Die Angreifer können unterschiedliche Angriffsmöglichkeiten haben (siehe Abbildung 12: Angriffsmöglichkeiten). Der Ausgangspunkt des Penetrationstests und der Umfang wird in Gesprächen im Vorfeld geklärt (siehe Abbildung 12: Angriffsmöglichkeiten).

Abbildung 12: Angriffsmöglichkeiten[69]



Allgemein werden vom BSI Audit-Techniken bevorzugt und nur vereinzelt Angriffe durchgeführt. Durch Gespräche mit dem Administrator sollen die internen Abläufe und Entscheidungen erklärt werden. Hierbei sollen schnell Fehlkonfigurationen, offene Zugänge oder Verbesserungspotenziale organisatorischer Abläufe erkannt werden. Die Administratoren erhalten direkt Feedback zu ihren Systemen und können die Verbesserungsvorschläge nach Abschluss des Tests gezielt verbessern. Das BSI möchte es vermeiden, dass es bei einem Test zu einem Ausfall kommt, daher werden Grundbedingungen, schützenswerte Geschäftsprozesse und Informationen identifiziert. Auf Grundlage der Netzpläne werden Schnittstellen ermittelt, über die ein Angriff erfolgen

[66] *BSI*, Ein Praxis-Leitfaden für IS-Penetrationstests, 2016, S. 5.
[67] Vgl. *BSI*, IS-Penetrationstest und IS-Webcheck.
[68] Vgl. *BSI*, IS-Webcheck., S. 1.
[69] Vgl. *BSI*, IS-Penetrationstest, 2018, S. 1.

könnte. Mit dieser Basis wird der Umfang des Tests festgelegt. Unter der Abgrenzung verdeutlicht das BSI, dass ein Penetrationstest nur eine Momentaufnahme ist und dass aufgrund der hohen Komplexität heutiger Informationsverbünde nicht garantiert werden kann, alle vorhandenen Schwachstellen aufzudecken. Es wird empfohlen Penetrationstests regelmäßig (z. B. alle zwei Jahre) zu wiederholen. Bei einer vom BSI durchgeführten Sicherheitsüberprüfung werden keine Methoden des Social Engineering eingesetzt.[70]

Zusammenfassende Erkenntnisse zum Thema Penetrationstest auf Grundlage der Dokumente vom BSI:

- Das Ziel ist es,
    - Schwachstellen zu identifizieren,
    - die Wirksamkeiten von Sicherheitsmaßnahmen zu prüfen und
    - das Angriffspotenzial auf ein IT-Netz, -System, -Anwendung zu testen.
- Der Penetrationstest ist
    - ein kontrollierter Eindringungsversuch in ein System oder Netzwerk.
    - vergleichbar mit einem realen Angriff.
    - wenig standardisierbar und zeitlich begrenzt.
- Die Ansatzpunkte sind IT-Systeme (z. B. Netzkoppelelemente, Server, Clients, usw.) oder (Web-)Anwendungen.
- Beim Penetrationstest werden keine Methoden des Social Engineering verwendet.
- Ein Penetrationstest ist eine Momentaufnahme und eine regelmäßige Prüfung wird empfohlen.
- Audit-Techniken werden vom BSI bevorzugt und nur in Einzelfällen Angriffe durchgeführt.

2.9.2 National Institute of Standards and Technology

Ein international anerkanntes Nachschlagewerk für Sicherheitstests ist der „*Technical Guide to Information Security Testing and Assessment 800-115*“ vom National Institute of Standards and Technology (NIST). Dort wird ein Penetrationstest wie folgt beschrieben:

> Penetration testing is a specialized type of assessment conducted on information systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Such testing can be used to either validate vulnerabilities or determine the degree of resistance organizational information systems have to adversaries within a set of specified constraints (e.g., time, resources, and/or skills). Penetration testing attempts to duplicate the actions of adversaries in carrying out hostile cyber attacks against organizations and provides a more in-depth analysis of security-related weaknesses/deficiencies. Organizations can also use the results of vulnerability analyses to support penetration testing activities. Penetration testing can be conducted on the hardware, software, or firmware components of an information system and can exercise both physical and technical security controls. A standard method for penetration testing includes, for example: (i) pretest analysis based on full knowledge of the target system; (ii) pretest identification of potential vulnerabilities based on pretest analysis; and (iii) testing designed to determine exploitability of identified vulnerabilities. All parties agree to the rules of engagement before the commencement of penetration testing scenarios.

[70] Vgl. *BSI*, IS-Penetrationstest, 2018., S. 1-4.

> Organizations correlate the penetration testing rules of engagement with the tools, techniques, and procedures that are anticipated to be employed by adversaries carrying out attacks. Organizational risk assessments guide decisions on the level of independence required for personnel conducting penetration testing.[71]

Zusammenfassende Erkenntnisse aus der Definition vom NIST:

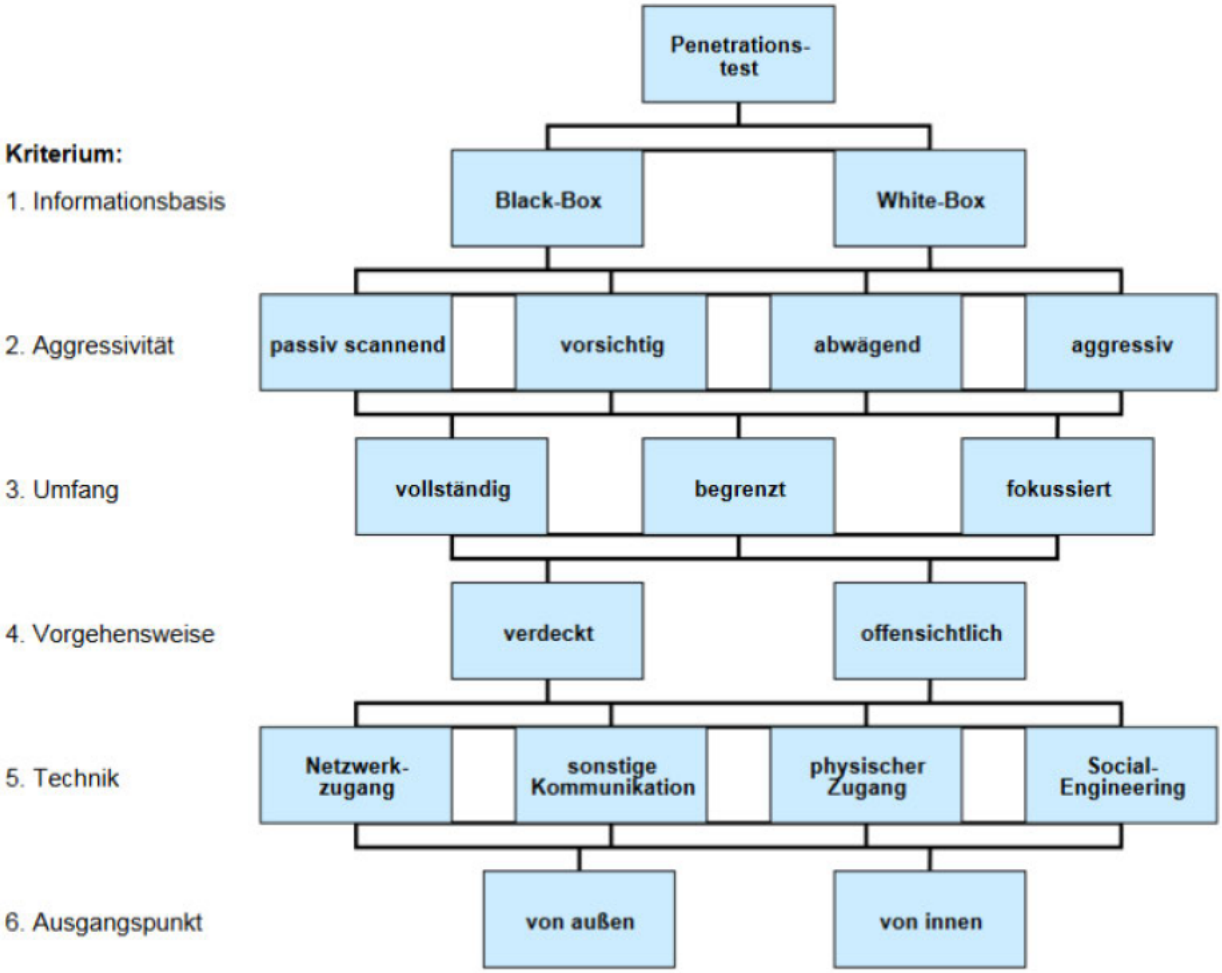
- Ein Penetrationstest
  - ist eine Art der Bewertung von Informationssystemen und einzelnen Systemkomponenten.
  - ist die Validierung von Schwachstellen oder Widerstandsgrad (Zeit, Ressourcen, Kenntnis) gegenüber Angreifern.
  - versucht Handlungen von Angreifern bei der Durchführung von Cyber-Angriffen nachzuahmen und eine vertiefte Analyse sicherheitsrelevanter Schwachstellen durchzuführen, um Sicherheitsmängel aufzudecken.
  - können an Hardware-, Software- oder Firmware-Komponenten durchgeführt werden.
  - kann sowohl physische als auch technische Sicherheitskontrollen überprüfen.
- Es ist eine Zustimmung zur Durchführung der Penetrationstest erforderlich.
- Die Tools, Techniken und Verfahren, die voraussichtlich eingesetzt werden, werden abgestimmt.
- Eine Standardmethode für ein Penetrationstest ist bspw. eine Pretest-Analyse auf Grundlage vollständiger Kenntnisse des Zielsystems, Identifikation von potenziellen Schwachstellen auf Basis der Pretest-Analyse und eine Prüfung, ob die identifizierten Schwachstellen ausnutzbar sind.
- Für die Durchführung und die Risikobewertung ist Unabhängigkeit erforderlich.

2.9.3 Klassifikation

Das BSI hat in der Studie „*Durchführungskonzept für Penetrationstest*“ einen Klassifizierungsbaum für Penetrationstests aufgebaut (siehe Abbildung 13: Klassifikation von Penetrationstests).

[71] *NIST*, NIST Special Publication 800-53 (Rev. 4).

Abbildung 13: Klassifikation von Penetrationstests[72]



In der folgenden Tabelle wird beschrieben, wie ein Penetrationstest klassifiziert und unterschieden werden kann.

Abbildung 14: Klassifizierung eines Penetrationstests[73]

Kriterium		Kurze Beschreibung
Informationsbasis Von welchem Wissensstand über das Objekt oder Netz geht der Tester aus?	White-Box	simuliert einen Angriff eines Insiders mit Detailkenntnissen
	Black-Box	simuliert einen Angriff ohne Kenntnisse über das Zielobjekt
Aggressivität Wie aggressiv geht der Tester vor?	passiv scannend	Systeme werden gescannt und mögliche Schwachstellen werden nicht ausgenutzt
	Vorsichtig	Die Schwachstellen werden nur dann ausgenutzt, wenn nach bestem Wissen eine Beeinträchtigung des Systems ausgeschlossen werden kann.

[72] Vgl. *BSI*, Studie Durchführungskonzept für Penetrationstests, S. 13.
[73] Vgl. *BSI*, Studie Durchführungskonzept für Penetrationstests, S. 13-17.

Kriterium		Kurze Beschreibung
	Abwägend	Es wird versucht, Schwachstellen auszunutzen, die unter Umständen zu Systembeeinträchtigungen führen können.
	Aggressiv	Es wird versucht, alle potenziellen Schwachstellen auszunutzen.
Umfang Welche Systeme sollen getestet werden?	vollständig	Alle erreichbaren Systeme werden geprüft.
	Begrenzt	Eine begrenzte Anzahl von Systemen oder Diensten wird untersucht.
	Fokussiert	Ein bestimmtes Teilnetz, System oder ein bestimmter Dienst wird geprüft.
Vorgehensweise Wie „sichtbar“ geht das Team beim Testen vor?	Verdeckt	Es kommen nur solche Methoden zum Einsatz, die nicht direkt als Angriffsversuch erkannt werden.
	offensichtlich	Auch Methoden, die offensichtlich erkannt werden können, werden verwendet, um Schwachstellen aufzudecken.
Technik Welche Techniken werden beim Testen eingesetzt?	Netzwerkzugang	Der Test wird über ein Netzwerk durchgeführt.
	sonstige Kommunikation	Der Test wird über weitere Kommunikationsnetze (z. B. WLAN) durchgeführt.
	physischer Zugang	Ein Tester hat physischen Zugang zum Testgegenstand.
	Social-Engineering	Verwendung von Social-Engineering-Techniken (z. B. Phishing)
Ausgangspunkt Von wo aus wird der Penetrationstest durchgeführt?	von außen	Der Test wird von außen, d. h. über das Internet durchgeführt.
	von innen	Der Test wird im internen Netzwerk durchgeführt

Ein Penetrationstest wird häufig als Black-Box-Test bezeichnet, da der Tester kein Wissen über das Zielobjekt hat. Aus rechtlichen und Effizienz-Gründen wird dem Tester die URL bzw. die IP-Adresse vom Testgegenstand oder den Testgegenständen übermittelt, damit diese nicht erst recherchiert werden müssen oder aber ein falsches Ziel angegriffen wird. Mit dieser Testweise soll typischerweise ein externer Angreifer simuliert werden, der nur unvollständiges Wissen über das Zielsystem hat.

2.9.4 Fazit

Ein Penetrationstest ist eine technische Sicherheitsüberprüfung, um die aktuelle Sicherheit von einem oder mehreren Assets (z. B. IT-Systemen oder (Web-)Anwendungen) zu prüfen. Die Prüfung geht von einem Auftraggeber aus und wird von diesem genehmigt und abgestimmt. Ein Penetrationstest wird in einer bestimmten Zeitspanne durchgeführt und

gibt eine Momentaufnahme über die IT-Sicherheit von einem oder mehreren Assets. Es wird empfohlen, diese regelmäßig durchzuführen. Das BSI hat in einer Studie beschrieben, wie ein Penetrationstest klassifiziert werden kann. Da Angreifer nicht einer bestimmten Vorgehensweise folgen, gibt es auch bei den Penetrationstester unterschiedliche Herangehensweisen. Zudem ist zu beachten, dass das Ergebnis von der Erfahrung, der Kreativität, der Vorgehensweise und den Fähigkeiten des Testers abhängig sind.

2.10 Red Teaming

> Red Teaming ist eine Methode, die im Militär des 19. Jahrhunderts entstanden ist, ursprünglich in der Ausbildung preußischer Offiziere. Man wollte damit die als Friktionen bezeichneten Unwägbarkeiten in militärischen Auseinandersetzungen besser beherrschen. Wetter, das Gelände, fehlende oder falsche Informationen, Probleme in der Versorgung, Verlagerung und Wirkung der eingesetzten Truppen, all dies hatte unkalkulierbare Auswirkungen auf den Erfolg eines ursprünglichen Plans. Historisch bedeutend ist das „taktische Kriegsspiel" des Barons von Reißwitz. Der ursprüngliche Apparat, im Berliner Schloss Charlottenburg zu besichtigen, war ein Brettspiel bestehend aus Terrainsteinen und Spielmarken mit dem, basierend auf einem detaillierten Regelwerk, Schlachtverläufe simuliert wurden. Zwei Parteien mussten, Zug um Zug, ihre Operationspläne durchsetzen. Jeder Zug hatte in exakt zwei Minuten zu erfolgen, angelehnt an die Dauer eines Artilleriefeuers. Neben der Entscheidung zum Einsatz der eigenen Truppen wurde der Verlauf des Gefechts durch Würfelspiele, stellvertretend für die unkalkulierbaren Friktionen, bestimmt. Diese ursprüngliche Methodik des Kriegsspiels wird heute zumeist als „War Game" bezeichnet und ist zum integralen Bestandteil des Planungsprozesses geworden. Ausgehend von der zeitlich begrenzten Analyse eines vorher ausgewählten Szenarios im Rahmen eines War Games, ist die Praxis des Red Teamings entstanden. Organisationen – neben dem Militär heute auch zivile Unternehmen – prüfen durch eigens dafür aufgestellte Red Teams ihre Annahmen und Pläne kritisch. Sie identifizieren Schwachstellen und erlangen ein besseres Verständnis ihres operativen Umfeldes, insbesondere im Cyber-Umfeld.[74]

Es gibt eine Vielzahl von Definitionen und Interpretationen zum Red Teaming. Das Ministry of Defence (MOD) aus Großbritannien beschreibt im Red Teaming Guide im Januar 2013 beispielsweise wie folgt:

> Red teaming is the independent application of a range of structured, creative and critical thinking techniques to assist the end user make a better informed decision or produce a more robust product.[75]

Was so viel bedeutet, dass Red Teaming die unabhängige Anwendung einer Reihe von strukturierten, kreativen und kritischen Denktechniken ist, die dem Endnutzer helfen, eine besser informierte/ fundiertere Entscheidung zu treffen oder ein robusteres Produkt zu entwickeln.

Die Aufgaben von Red Teaming sind:

- Die eigenen Pläne, Programme, Behauptungen und Annahmen bewusst in Frage zu stellen, um fehlerhafte Logik oder Analysen zu identifizieren.
- Ein System, einen Plan oder eine Perspektive mit den Augen eines Gegners, Außenseiters, Konkurrenten oder Mitbewerbers zu testet und zu fordern.

[74] *Deloitte*, Red Team., S. 7
[75] *Ministry of Defence*, Red Teaming Guide, 2013., S. 3.

- Es sollen die einem Gegner zur Verfügung stehenden Möglichkeiten verstanden werden, indem plausible Annahmen über das gegnerische Verhalten getroffen werden, um so dem Gegner entgegen zu wirken.
- Die Perspektiven und wahrscheinlichen Handlungen für von Partner, Einheimischen und anderer einflussreicher Akteure verstehen.
- Es soll ein besseres Verständnis für Partner, Einheimischen und anderer einflussreicher Akteure entstehen.
- Es bereitet eine Organisation darauf vor, mit Überraschungen und strategischen Schocks umzugehen und sie abzuschätzen.
- Die Stärke von Beweisen oder die Qualität der Informationen wird beurteilt.
- Die alternativen Optionen oder Ergebnisse identifizieren und/oder die Folgen einer bestimmten Vorgehensweise zu untersuchen.[76/77]

Red Teaming wurde vom Militär auf den Bereich der Cyber Security übertragen. Hierzu wurden mehrere Frameworks veröffentlicht, die in den folgenden Kapiteln betrachtet werden.

2.10.1 SANS Red Teaming: The Art of Ethical Hacking

Das SysAdmin, Networking and Security (SANS) Institut wurde 1989 als Forschungs- und Bildungsorganisation gegründet. Sie entwickelt, pflegt und stellt kostenlos eine Sammlung von Forschungsdokumenten zu verschiedenen Aspekten der Informationssicherheit zur Verfügung.[78] Von SANS wurde im Dezember 2003 ein Dokument veröffentlicht, welches die Notwendigkeit von Red Teaming beschreibt. Die folgenden Ausführungen sind aus dem Whitepaper entnommen.[79]

Im Whitepaper wird beschrieben, dass bereits seit 2003 die Wirtschaft und nationale Sicherheit vollständig von der Informationstechnologie und -infrastruktur abhängig sind. Ein Netzwerk unterstützt direkt den Betrieb aller Sektoren unserer Wirtschaft. Jedes dieser Netzwerke überschreitet mittlerweile die Grenzen. Zudem werden auch physikalische Objekte wie z. B. elektrische Transformatoren, Züge, usw. gesteuert. Angreifer führen Angriffe auf kritische Informationsinfrastrukturen durch. Von größter Bedeutung ist die Bedrohung durch organisierte Angriffe, die in der Lage sind, die kritischen Infrastrukturen, die Wirtschaft oder die nationale Sicherheit der Nation zu gefährden. Angriffe auf US-amerikanische Informationsnetzwerke können schwerwiegende Folgen haben, wie z. B. die Unterbrechung kritischer Abläufe, den Verlust von Einnahmen und geistigem Eigentum oder den Verlust von Menschenleben. Gegen solche Angriffe bedarf es der Entwicklung von neuen Methoden, um Schwachstellen zu reduzieren und Angreifer davon abzuhalten, Angriffe auf kritische Infrastrukturen durchzuführen. Red Teaming ist ein Prozess, der entwickelt wurde, um Netzwerk- und Systemschwachstellen zu erkennen und die Sicherheit zu testen. Mit dem

[76] Vgl. *Ministry of Defence*, A Guide to Red Teaming, 2013., S. 4-5.
[77] Vgl. *Ministry of Defence*, Red Teaming Guide, 2013., S. 5-6.
[78]Vgl. *SANS*, About.
[79] Vgl. *Peake, C.*, Red Teaming: The Art of Ethical Hacking, 2003.

Whitepaper sollte die Notwendigkeit solcher Methoden gerechtfertigt werden, um ein Bewusstsein für Netzwerk-/ Systemsicherheit zu schaffen.

Informationssicherheitsexperten können in Red und Blue Teams aufgeteilt werden. Red Teaming ist der Prozess der Analyse von Schwachstellen auf einem bestimmten System oder Netzwerk durch das Durchführen von Angriffen eines Gegners. Das Blue Teaming ist der Prozess der Verteidigung. Hierbei wird mit den Netzwerk- oder Systembetrieb zusammengearbeitet, um Angriffe zu erkennen und Risiken zu minimieren. Die Ansätze identifizieren bekannte Schwachstellen auf Systeme, aber nicht die Anforderungen an eine übergreifende Sicherheitsinfrastruktur. Informationssicherheit ist eine Denkweise und ein rotierender Prozess. Das Red Teaming ist eine Komponente bei der Bewertung der Sicherheit eines Netzwerks und Systems. Durch die Bewertung beim Red Teaming können das Risiko eines Systems oder Netzwerk ermittelt und Sicherheitsmaßnahmen abgeleitet werden. Um das Risiko zu bestimmen, werden Schwachstellen und Bedrohungen identifiziert.

Das Red Team nutzt hierzu Tools, um in einem vom Kunden gewünschten Umfang nach Schwachstellen zu suchen und mögliche Bedrohungen aufzudecken. Der Red Teaming-Ansatz reicht tiefergehender als die Vorstöße der meisten potenziellen Angreifer, die jeweils versuchen, Sicherheitsvorkehrungen zu umgehen und eine einzige Schwachstelle zu finden. Sicherheitsexperten versuchen, möglichst alle Schwachstellen für ein bestimmtes System zu finden, um das damit verbundene Risiko bewerten zu können. Ein Angreifer zielt typischerweise in der Regel auf eine einzelne Schwachstelle mit einem bestimmten Exploit ab, da der Angreifer die Gefahr zur Erkennung reduzieren will. Je mehr Zeit ein Angreifer damit verbringt, ein System oder Netzwerk nach Schwachstellen zu untersuchen, desto höher ist die Gefahr, dass der Angriff erkannt wird.

Das Red Teaming sollte im Vergleich zu einem realen Angriff mehrere Arten von Angriffen testen, um eine Sicherheitsbewertung über Sicherheitslage eines Systems oder Netzwerk zu erhalten. Die Identifikation von Risiken durch Red Teaming und anderen Methoden allein bietet keine allgemeine Informationssicherheit. Das Unternehmen muss einen kontinuierlichen Informationssicherheitsprozesse betreiben, um Risiken angemessen zu verwalten und einen Schutz der Informationssicherheit zu gewährleisten.

Red Team Assessment (dt. Bewertung) bewertet verschiedene Sicherheitsbereiche in einem mehrstufigen Ansatz (engl. multi-layered approach / engl. Defense in Depth). In jedem Bereich wird das Ziel (System oder Netzwerk), welches bewertet wird, festgelegt. Anschließend wird das Ziel bzw. die Einhaltung der Sicherheitsmaßnahmen auf jeder Ebene im Defense in Depth-Konzept auf mögliche Angriffe und Eindringungsmöglichkeiten überprüft. Jede Sicherheitsmaßnahme wird auf eine Art und Weise getestet, die dafür Sinn macht.

Ein Red Teaming Assessment muss mit größter Vertraulichkeit, Diskretion und Klarheit durchgeführt werden. Typischerweise werden für Red Teams Dienstleister beauftragt,

damit eine unparteiische und unvoreingenommenen Bewertung durchgeführt wird. Bei der Auswahl des Dienstleisters ist Vorsicht geboten. Ein richtig ausgewähltes Team liefert ein gutes Ergebnis für die Sicherheit und reduziert den Aufwand der Firma, aber ein falsch ausgewähltes Team kann einen Schaden an der Sicherheit, der Reputation und der IT-Infrastruktur anrichten.

Der Kunde legt den Umfang des Projekts fest, welcher den Bereich mit den zu bewertenden Informationen beinhaltet. Bevor das Red Teaming startet, müssen rechtliche Aspekte berücksichtigt werden. Damit das Red Teaming beginnen kann, muss eine ausdrückliche und direkte Erlaubnis zur Durchführung des Tests durch den Kunden vorliegen. Diese Erlaubnis sollte eine Verzichtserklärung im Falle einer im Testverlauf möglichen Katastrophe beinhalten. Das Red Team ist dafür verantwortlich dem Kunden einen detaillierten Plan sowie eine Liste von Methoden und Tools zur Verfügung zu stellen, die während der Evaluierung eingesetzt werden. Alle Tests, die außerhalb des vom Kunden angegebenen Umfangs durchgeführt werden, können als ungerechtfertigter Angriff des Red Teams angesehen werden. Der Kunde behält die Rechte an urheberrechtlich geschützten Daten und Information. Zu keinem Zeitpunkt sollte die Vertraulichkeit oder Verfügbarkeit dieser Informationen durch den Test gezielt gefährdet werden.

Unter den Ethical Hacker gibt es einen umfangreichen Werkzeugkasten aus Software, Hardware und technischem Fachwissen. Die wahre Stärke beim Red Teaming besteht darin, die Tools und Techniken anwenden zu können. Bei jedem Bereich der Schwachstellenbewertung werden spezifische Tools benötigt, um die Sicherheitskonfiguration zu überprüfen. Hierbei kann das Red Team Experten in unterschiedlichen Fachbereichen haben, da sich die Fähigkeiten, die benötigt werden, bspw. um Social-Engineering Angriffe durchzuführen, erheblich von anderen Themenbereichen unterscheiden können. Daher besteht das Red Team häufig aus mehreren versierten Personen, die Spezialisten auf einem der folgenden Fachgebiete sind:

- Entwicklung eines Hacker's Mind
- Port Scanning
- Network Surveying
- Systemidentifikation / OS Fingerprinting
- Schwachstellenforschung und Verifikation (automatisiert und manuell)
- Implementierung der richtigen Tools für jede Aufgabe im Sicherheitstest
- Dienste identifizieren
- Exploiting von Schwachstellen / Exploit-Forschung
- Webanwendungstests
- Festlegung geeigneter Gegenmaßnahmen zur Verhinderung von bösartigen Hacking-Angriffen
- Dokumentenanalyse
- Durchführung von Rechtsgutachten

- Untersuchung eines Unternehmens auf Schwächen wie aus der Sicht eines Industriespions oder eines Wettbewerbers
- Firewall & Access Control List (ACL) Tests
- Intrusion Detection System (IDS) Tests
- Social Engineering
- Passwort Knacken
- Denial-of-Service Tests

Die Kombination aus Tests aus unterschiedlichen Gebieten wird in die Sicherheitsbewertung die das Red Teaming liefern, einbezogen. Für die unterschiedlichen Tests gibt es eine Vielzahl von Tools, die vom Tester ausgewählt werden. Die Auswahl der Tools sollte aber auf Grundlage der identifizierten Angreifer erfolgen, die durch die Bedrohungsanalyse ermittelt wurden. Das Red Team simuliert einen realen Angriff. Dabei ist zu beachten, dass, wenn als Angreifer konkurrierende Unternehmen mit großen finanziellen Ressourcen vorhanden sind, die Auswahl der Tools eine andere ist, als wenn die Angreifer-Gruppe Script-Kiddies identifiziert wurde.

Red Teaming ist ein methodischer Prozess, der ein bestehendes Sicherheitsniveau bewertet und dabei helfen soll, das Verständnis von Bedrohung, Schwachstelle und Risiko zu verbessern. Die Rolle des Red Teaming besteht darin, den Kunden ein Bewusstsein dafür zu vermitteln, wie sie potenziell angegriffen werden können und warum sie angegriffen werden.

2.10.2 NIST Red & Blue Team Ansatz

In der *„NIST Special Pulication 800-161“* von April 2015 wird ein Red und Blue Team-Ansatz beschrieben. Bei diesem Ansatz versucht eine autorisierte und organisierte Gruppe von Personen Angriffs- oder Exploit-Fähigkeiten eines potenziellen Angreifers anzuwenden, um den Sicherheitszustand eines Unternehmens zu prüfen. Das Ziel des Red Teams ist es, die Informationssicherheit im Unternehmen zu verbessern, indem die Auswirkungen erfolgreicher Angriffe verdeutlicht werden und aufgezeigt was bei der Verteidigung (d. h. das Blaue Team) in einer operativen Umgebung funktioniert. Der Ansatz hat folgende Eigenschaften:

- Tests werden typischerweise über einen längeren Zeitraum durchgeführt
- Tests werden in einem repräsentativen Kontext (z. B. durch operative Übungen) ausgeführt
- mit Hilfe einer neutralen Gruppe (White Team) werden die Simulationen und Übungen festgelegt und überwacht

Das Blue Team ist eine Gruppe von Personen, die Schwachstellen im operativen Netzwerk bewertet und Mitigation-Techniken für den Kunden bereitstellt. Die Gruppe prüft unabhängig die technische Sicherheitslage. Sie identifiziert Sicherheitsbedrohungen und -risiken im Betriebsumfeld und analysiert in Zusammenarbeit mit dem Kunden die Netzwerkumgebung und den aktuellen Stand der Sicherheitslage. Basierend auf den

Erkenntnissen und dem Fachwissen des Blue Teams liefern sie Empfehlungen, die sich in eine allgemeine Sicherheitslösung integrieren lassen, um die Cyber-Sicherheit des Kunden zu erhöhen. Häufig wird ein Blue Team allein oder vor einem Einsatz eines Red Teams bereits eingesetzt, um sicherzustellen, dass die Netzwerke des Kunden so sicher wie möglich sind, bevor das Red Team die Systeme testet.[80]

2.10.3 Microsoft Enterprise Cloud Red Teaming

Microsoft hat am 25.02.2016 ein Whitepaper mit dem Titel „*Microsoft Enterprise Cloud Red Teaming*“ veröffentlicht. In diesem Whitepaper wird die Strategie und Durchführung von Red Teaming auf Microsoft Managed Cloud Infrastrukturen, Services und Anwendungen erläutert. Auf dieses Whitepaper wird im Folgenden eingegangen.[81]

> Fundamentally, if somebody wants to get in, they are getting in… Accept that. What we tell client is: Number one, you‘re in the fight, whether you thought you were or not. Number two, you almost certainly are penetrated.
>
> *Michael Hayden (ehemaliger Direktor der NSA & CIA)*

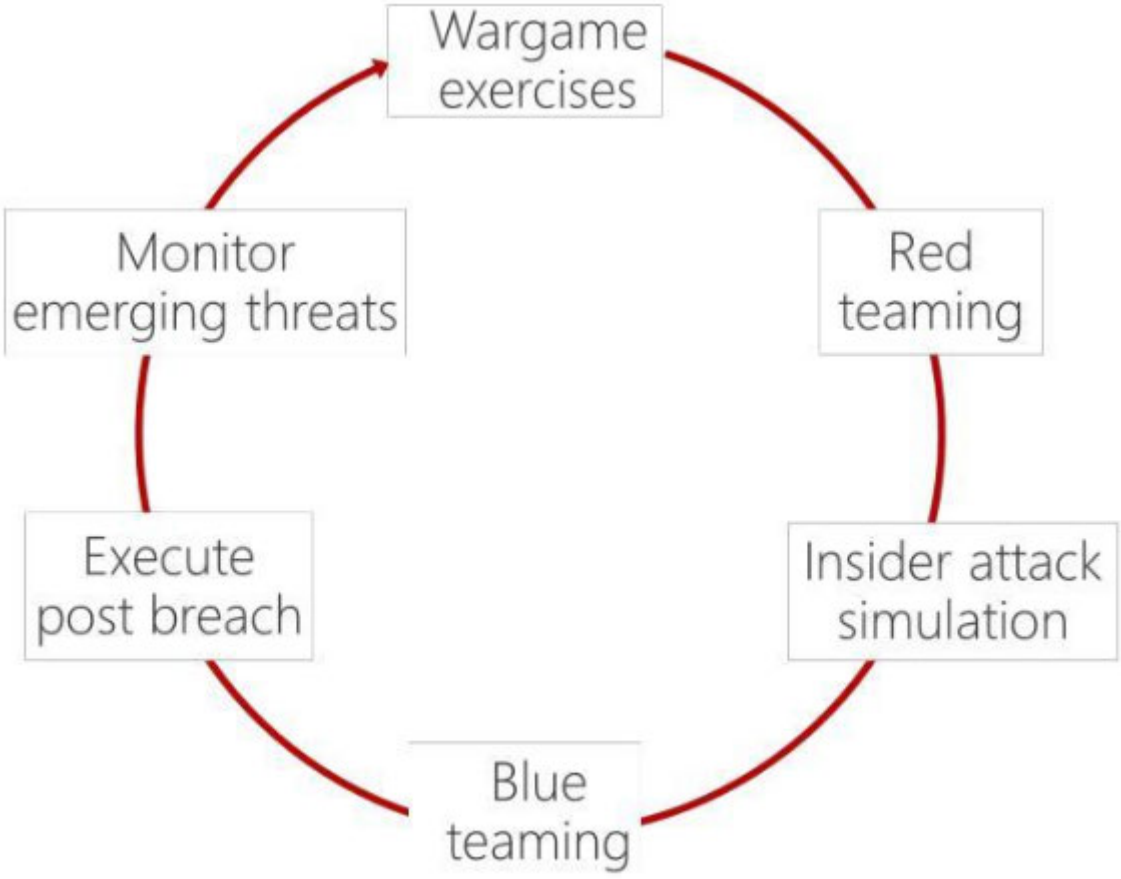
Das bedeutet ganz grundsätzlich, dass jemand reinkommen wird, wenn er reinkommen will. Akzeptiere das! Was wir dem Kunden sagen, ist: Nummer eins, du bist im Kampf, ob du daran gedacht hast, dass du es bist oder nicht. Nummer zwei, du wirst mit ziemlicher Sicherheit penetriert.

Unternehmen können sich besser auf die Auswirkungen aktueller und zukünftiger Bedrohungen vorbereiten, wenn sie reale Angriffe simulieren und dabei Taktiken, Techniken und Verfahren (TTPs) von Angreifern bei Sicherheitsvorfällen einsetzen. Anstatt das Auftreten zu verhindern, ist es wichtig, anzunehmen, dass ein Sicherheitsvorfall eintreten kann und wird. Dies wird durch das Zitat von Michael Hayden hervorgehoben.

Unternehmen können sich nicht umfassend vor Schwachstellen schützen. Daher muss sich ein Unternehmen mit der Detektion und Reaktion auf Sicherheitsverstöße auseinandersetzen. Durch die Planung von Worst-Case-Szenarien, durch Wargames (Tabletop-Angriff) und Red Teaming (Real-World-Angriff) können Unternehmen die notwendigen Fähigkeiten entwickeln, um Eindringungsversuche zu erkennen und die Reaktionen im Zusammenhang mit Sicherheitsverletzungen deutlich zu verbessern. Die Maßnahmen werden in einem Zyklus durchgeführt (siehe Abbildung 15: Zyklus zum Training für einen Sicherheitsvorfall).

[80] Vgl. *NIST*, Red Team/Blue Team Approach.
[81] Vgl. *Microsoft*, Microsoft Enterprise Cloud Red Teaming, 2014.

Abbildung 15: Zyklus zum Training für einen Sicherheitsvorfall



Beim Red Teaming werden zwei Gruppen gebildet. Das Red Team ist Angreifer und das Blue Team Verteidiger. Das Red Team verwendet gleiche TTPs wie reale Angreifer und führt Tests gegen die Live-Produktivinfrastruktur durch. Das Blue Team, das zum Beispiel aus dem Infrastruktur-, Plattform-Engineering- oder Betriebs-Team besteht, wird nicht darüber informiert. Dadurch soll die Sicherheitserkennungs- und Reaktionsfähigkeit vom Blue Team getestet werden und dabei helfen Schwachstellen im Produktivsystem, Konfigurationsfehler und andere Sicherheitsprobleme zu identifizieren. Nach jedem Vorstoß des Red Teams folgt eine vollständige Aufdeckung, um Schwachstellen zu identifizieren, zu adressieren und die Reaktion auf einen Sicherheitsvorfall zu verbessern. Die Informationen, die durch Red Teaming gewonnen werden, helfen, die Verteidigung deutlich zu stärken, die Reaktionsstrategien zu verbessern, die Verteidiger auszubilden und die Effektivität des gesamten Sicherheitsprogramms zu erhöhen.

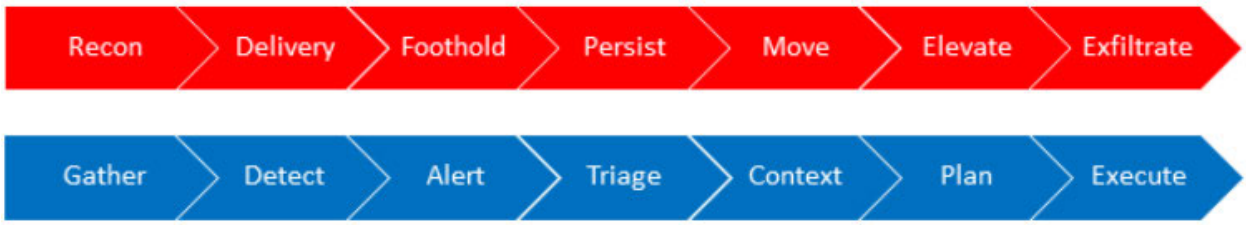
Bei Microsoft sind im Red Team Vollzeitmitarbeiter, die sich darauf konzentrieren, in eine Infrastruktur einzudringen. Sie sind die Angreifer, die gezielt und anhaltend Angriffe auf Microsoft Online Services (Microsoft, Infrastruktur, Plattformen, Anwendungen) durchführen. Die Erforschung und das Verständnis von Sicherheitsvorfällen in der Branche und Trends in der Bedrohungslandschaft ist ebenfalls eine der Aufgaben des Red Teams. Es

hat die große Herausforderung, immer auf dem neusten Stand der Angriffstechniken und -Werkzeuge der Gegner zu bleiben.

Das Blue Team besteht meistens aus Sicherheitsbeauftragten, Mitarbeiter des Security Incident Response, der Entwicklung und des Betriebs. Unabhängig von der Zusammensetzung arbeiten sie getrennt vom Red Team. Beim Blue Team werden etablierte Sicherheitsprozesse umgesetzt, vorhandene Tools und Technologien verwendet, um Angriffe zu erkennen und darauf zu reagieren. Genau wie bei einem realen Angriff weiß das Blue Team nicht, wann und wie die Angriffe stattfinden oder welche Methoden eingesetzt werden. Das Ziel ist es, Angriffe zu erkennen und darauf zu reagieren, egal ob es sich vom Red Team oder einem realen Angriff handelt. Wenn ein Angriff erkannt wird, muss das Team:

- Beweise, die der Angreifer hinterlassen hat, sammeln,
- Beweise als Indikator einer Kompromittierung erkennen,
- die zuständigen Entwicklungs- und Betriebsteams alarmieren,
- Warnmeldungen auswerten, um festzustellen, ob eine weitere Untersuchung notwendig ist,
- den Zusammenhang des Sicherheitsvorfalls erfassen,
- einen Behebungsplan erstellen, um den Angriff einzudämmen oder zu verhindern und
- den Behebungsplan und die Wiederherstellung durchführen.

Abbildung 16: Prozess Vergleich Red und Blue Team



Die Abbildung zeigt die Schritte des Blue Teams verglichen mit dem Red Team. Das Ziel des Blue Teams ist es, die Angriffe des Red Teams von Anfang bis Ende nachvollziehen zu können, um dies bei einem realen Angriff ebenfalls zu können. Es soll vorgegangen werden wie beim realen Angriff, um dies zu praktizieren und ein Bewusstsein, wie mit der Situation umzugehen ist, zu schaffen. Das Red Team weiß nicht, was das Blue Team macht und umgekehrt. Beim Red Teaming kann das Red Team im Prozess unbeabsichtigt oder beabsichtigt einen Sicherheitsvorfall auslösen. Eine absichtliche Warnmeldung kann vom Red Team ausgelöst werden, um herauszufinden, ob der Angriff erkannt wurde. Durch Abstimmung zwischen Red und Blue Team nach einem erfolgreichen Angriff soll die Erkennung und Reaktion kontinuierlich verbessert werden. In einer nachfolgenden Analyse werden die Reaktion bewertet und die Details zwischen den Teams ausgetauscht.

Im Gegensatz zu herkömmlichen Penetrationstests versucht das Red Teaming eine reale Bedrohung inklusive des "*Fog of war*" (dt. Nebel des Krieges / Kriegsnebel) zu simulieren. Der Ausdruck "*Fog of war*" bezeichnet die Unsicherheit, die Organisationen für bestimmte

Situationen haben. Theoretische Angriffsszenarien werden beim Red Teaming real. Es werden Schwachstellen ausgenutzt, Schwächen aufgedeckt und konkrete Nachweise für die notwendigen Vorgehensweisen bei einem Sicherheitsvorfall geliefert. Durch Red vs. Blue Team Übungen werden Security Organisationen auf die wichtigsten Angriffsvektoren hintrainiert, Gegenmaßnahmen entwickelt und Reaktionsmechanismen zur Vorbereitung auf gezielte und persistente Angreifer ausgereift.

Die wichtigen Sicherheitsprinzipien, die Microsoft aus Red Teaming gelernt hat, sind:

- Es gibt keine statischen Angriffsszenarien und die Angreifer kommen nicht nur von einer festen Position.
- Es müssen ergänzende Schichten von Maßnahmen verwendet werden, aus der eine kumulierte Auswirkung auf die Verbesserung der Verteidigung entsteht.
- Die Anzahl und Verteilung der Sicherheitsmaßnahmen sind wichtiger als die individuelle Effizienz.
- Es muss versucht werden, den Angriff zu verzögern und darauf zu reagieren, anstatt ihn zu verhindern.

Microsoft führt regelmäßig Red Teaming durch und ist davon überzeugt, dass die heutige Bedrohungslandschaft dies notwendig macht, da die durchschnittliche Zeit bis zur Erkennung und Wiederherstellung nach einem Sicherheitsvorfall erheblich verkürzt werden sollte.

2.10.4 CBEST Framework

Das Council of Registered Ethical Security Testers (CREST) ist eine gemeinnützige Non-Profit-Akkreditierungs- und Zertifizierungsstelle mit Sitz in England, die im Markt der Informationssicherheit tätig ist.[82] CREST hat in Zusammenarbeit mit der Bank of England das CBEST Framework entwickelt. Die zweite Version wurde 2016 veröffentlicht. Im Leitfaden des Frameworks wird erklärt, was Red Teaming ist, was man am besten daraus macht und welche Vorteile es mit sich bringt.[83]

CBEST ist auf den Finanzsektor ausgerichtet. Es beschreibt die Durchführung von kontrollierten, maßgeschneiderten, intelligent gesteuerten Cyber-Sicherheitstests. Die Tests replizieren das Verhalten von Bedrohungsakteuren, die von Regierungen und kommerziellen Nachrichtendiensten als echte Bedrohung für systemrelevante Finanzinstitute bewertet werden. CBEST unterscheidet sich von anderen Sicherheitstests, die derzeit im Finanzdienstleistungssektor durchgeführt werden, dadurch, dass es auf Bedrohungsinformationen basiert, weniger eingeschränkt ist und sich auf die komplexeren und anhaltenderen Angriffe auf kritische Systeme und wesentliche Dienste konzentriert. CBEST bietet eine ganzheitliche Bewertung der Cyberfähigkeiten eines Finanzdienstleisters oder Infrastrukturanbieters, indem es Menschen, Prozesse und Technologien in einem

[82] Vgl. *CREST*, Assurance in Information Security, 2019.
[83] Vgl. *CREST*, An introduction to CBEST.

einzigen Test prüft. Die Einbeziehung spezifischer Cyber-Bedrohungsinformationen stellt sicher, dass die Tests, die sich entwickelnde Bedrohungslandschaft so genau wie möglich nachbilden und daher relevant bleiben.

Bei CBEST werden Kennzahlen verwendet, um die Leistungsfähigkeit und Reife zu messen und der Branche und den Regulierungsbehörden Benchmark-Informationen zur Verfügung zu stellen. Die Benchmark-Informationen verbessern nicht nur die Organisationen, die CBEST anwenden, sondern tragen auch dazu bei, herauszufinden, in welchen Bereichen Unternehmen der Finanzdienstleistungsbranche den Aufwand erhöhen müssen, sich vor Cyberangriffen zu schützen und angemessen zu reagieren.

CREST verlangt von den Unternehmen die Sicherheitstests nach Ihrem Standard durchführen, dass diese über bestimmte Richtlinien und Prozesse zur Verwaltung und Durchführung von CBEST-Aktivitäten verfügen und nachgewiesen können. CREST verlangt auch die Akkreditierung von Threat Intelligenz Anbietern, um sicherzustellen, dass Anbieter von Finanzdienstleistungen und Infrastrukturen Zugang zu detaillierten, durchdachten und konsistenten Cyber-Bedrohungsinformationen haben, die aus ethischen und rechtlichen Gründen gewonnen wurden. Das CBEST-Framework stellt sicher, dass Sicherheitstester und Anbieter von Bedrohungsinformationen zusammenarbeiten und sehr reale Angriffe von erfahrenen Gegnern replizieren. Sowohl die Unternehmen, die CBEST-Dienstleistungen erbringen, als auch die für die Durchführung der Arbeiten qualifizierten Unternehmen, sind an detaillierte, relevante und durchsetzbare Verhaltenskodizes gebunden, die von CREST verwaltet werden.[84] Im CBEST-Framework wird auch ein Penetrationstest durch eine Threat Intelligence Phase ergänzt.[85]

CREST hat im April 2017 einen Leitfaden für die Durchführung eines effektiven Penetrationstestprogramms veröffentlicht. In diesem wird unter anderem Red und Blue Teaming definiert. Zudem wird beschrieben, dass sich viele Sicherheitsbewertungen auf die Breite und nicht auf die Tiefe konzentrieren, sowie auf eine zu testende Komponente beschränkt sind. Red Teaming ist dagegen eine zielorientierte Bewertung, die einen Einblick in die Praxis gibt, was ein Angreifer tun würde, um die Vermögenswerte Ihrer Organisation zu gefährden. Ein Red Teamer wird sich nicht nur auf Ihre Netzwerkinfrastruktur oder Webanwendungen konzentrieren.

Organisationen bilden Red Teams, um Aspekte ihrer eigenen Pläne, Programme und Annahmen in Frage zu stellen. Es ist dieser Aspekt der bewussten Herausforderung, der das Red Teaming von anderen Managementinstrumenten unterscheidet, obwohl es keine scharfe Grenze zwischen ihnen gibt. Heutzutage kommt Red Teaming oft von einem intelligent geführten Penetrationstest-Ansatz, der darauf abzielt, die Abwehrkräfte einer Organisation in realen Szenarien gründlicher zu testen. Obwohl es nur wenige Definitionen

[84] Vgl. *CREST*, About CREST, 2019.
[85] Vgl. *CREST*, CBEST Intelligence-Led Testing.

von Blue Teaming gibt, spielt ein Blue Team typischerweise die Rolle der Verteidigung gegen Angriffe des Red Team. Unternehmen sollten die Notwendigkeit von Red und Blue Teaming in ihren Unternehmen als Teil ihres Penetrationstestprogramms berücksichtigen.[86]

2.10.5 TIBER-EU Framework

Im Mai 2018 wurde das „*Framework for Threat Intelligence-based Ethical Red Teaming*" (TIBER-EU) von der europäischen Zentralbank veröffentlicht, um Finanzinfrastrukturen und -institutionen vor anspruchsvollen Cyberangriffen zu schützen. In diesem Framework wird die Vorgehensweise des Red Teaming beschrieben. Die folgenden Ausführungen sind aus dem Dokument „*How to implement the European framework for Threat Intelligence-based Ethical Red Teaming*".[87]

Das TIBER-EU soll europäischen und nationalen Behörden ermöglichen, mit Finanzinfrastrukturen und Institutionen ein Programm zum Testen und Verbessern der Widerstandsfähigkeit gegen komplexe Cyber-Angriffe aufzubauen. TIBER-EU ist ein Framework, das einen kontrollierten, maßgeschneiderten, intelligent geführten Red Team Test für kritische Live-Produktivsysteme von Unternehmen beschreibt. Das Red Team imitiert Taktiken, Techniken und Verfahren (engl. Tactics, Techniques and Procedures (TTP)) von realen Bedrohungen für das Unternehmen. Der Ansatz soll einen Angriff auf die kritischen Funktionen (engl. criticial function (CF)) und zugrunde liegenden Systemen, d. h. Mitarbeiter, Prozesse und Technologien simulieren. Das Framework soll dabei helfen die Schutz-, Erkennungs- und Reaktionsfähigkeit von Unternehmen zu bewerten. Die Kern-Ziele sind:

- Verbesserung der Widerstandsfähigkeit von Unternehmen gegen Cyber-Angriffe
- Standardisierung und Harmonisierung der Art und Weise, wie Unternehmen Red Team Tests in der Europäischen Union durchführen. Das Framework bietet dabei ein gewisses Maß an Flexibilität, um das Framework auf Besonderheiten anzupassen.
- Es soll den Behörden eine Leitlinie zur Hand geben, wie eine Prüfung auf nationaler und europäischer Ebene eingeführt, durchgeführt und verwaltet werden kann.
- Es unterstützt grenz- und rechtsübergreifende Red Team Tests für multinationale Unternehmen.
- Ermöglicht Diskussionen über die Bewertung bei eine TIBER-EU Test. Der Regulierungsaufwand für Unternehmen wird verringert und ein anerkanntes Testverfahren in der gesamten EU gefördert.
- Beim Test wird ein Bericht für die behörden- und grenzübergreifende Zusammenarbeit, den Ergebnisaustausch und die Analyse wird erstellt.

Bei einem Red Team Test nach dem TIBER-EU werden alle TTP von Advanced Thread Actors, die als eine reale Bedrohung für ein Unternehmen wahrgenommen werden, betrachtet. Ein Red Team Test soll mit einer Vielzahl von Techniken einen Angriff entweder durch

[86] Vgl. *CREST*, A guide for running an effective Penetration Testing programme, 2017.
[87] Vgl. *ECB*, TIBER-EU Framework, 2018.

böswillige Außenstehende oder durch interne Mitarbeiter simulieren und so alle Vorkehrungen, die von einem Unternehmen bezüglich Informationssicherheit getroffen wurden, inklusive Menschen, Prozesse und Technologien testen.

Bei einem Test sind folgende Akteure beteiligt:

- staatliche Geheimdienste oder nationale Cyber Security Centre
- TIBER-Cyber-Team (TCT)
- TIBER-EU Knowledge Centre (TKC)
- White Team (WT) und White Team Lead (WTL)
- Thread Intelligence (TI) Provider
- Blue Team (BT)
- Red Team (RT) Provider

In vielen Staaten kann es einen Geheimdienst, ein nationales Cybersicherheitszentrum oder Ähnliches geben. In solchen Rechtsordnungen können die Behörden beschließen, mit diesen Stellen zusammenzuarbeiten und sie in den Prozess einzubeziehen. Der Geheimdienst oder das Cybersicherheitszentrum kann Einblick in den Prozess der Bedrohungsaufklärung geben und versuchen, die einzelnen Targeted Threat Intelligence (TTI)-Berichte mit ihrem internen Wissen zu bereichern. Es liegt im Ermessen der nationalen Behörden, die Rolle des Nachrichtendienstes oder des Cybersicherheitszentrums zu bestimmen und die entsprechenden Maßnahmen zur Interaktion mit ihnen zu ergreifen.

Die Behörden, die sich für eine Umsetzung von TIBER-EU entscheiden, müssen ein zentrales TCT einrichten. Das TCT soll als zentrale Anlaufstelle zwischen nationaler und europäischer Ebene dienen. Es unterstützt die WTL, die verantwortlich für das Testmanagement in einer Institution sind, mit Fachwissen. Das TCT ist auch für die Pflege des nationalen und europäischen TIBER-Implementierungsleitfadens und dessen Weiterentwicklung nach nationalen oder europäischen Bedürfnissen verantwortlich. Darüber hinaus können nationale und europäische TCTs mit anderen in unterschiedlichen Ländern, in denen das TIBER umgesetzt wird, zusammenarbeiten.

Von der EZB wurde ein TIBER-EU Knowledge Centre (TKC) eingerichtet, das die Zusammenarbeit zwischen nationalen und europäischen TCT erleichtern soll. Die Ziele vom TKC sind:

- Wissensaustausch erleichtern und Zusammenarbeit zwischen nationalen und europäischen TCTs fördern.
- Unterstützung nationaler und europäischer Implementierung und ein zentrales Depot für gerichtliche Materialien zur Verfügung stellen.
- Den Behörden Schulungen über die Entwicklung, Durchführung und Verwaltung des TIBER-EU-Rahmens anbieten.
- Die nationalen und europäischen Implementierungen überwachen, Feedback sammeln, gewonnene Erkenntnisse reflektieren, gegebenenfalls nationale

Gerichtsbarkeiten informieren, das TIBER-EU-Framework aufrechterhalten und kontinuierlich weiterentwickeln.
- Förderung des Informationsaustausches, der gegenseitigen Zusammenarbeit und anderer Maßnahmen zur Verbesserung der allgemeinen Cyber Widerstandsfähigkeit innerhalb der EU.
- Kontakt mit anderen Behörden zur Förderung der internationalen Vereinheitlichung und Qualität aufnehmen.
- Rückmeldung an den Sektor innerhalb relevanter Foren z. B. dem Euro Cyber Resilience Board für die paneuropäische Finanzinfrastruktur, falls erforderlich und angemessen.

Die zwei Hauptakteure für das Projektmanagement des Tests sind das TCT der Behörde und das WT der Organisation. Beide sollten umfassende Kenntnisse über das Geschäftsmodell, die Funktionen und über die Dienstleistung verfügen. Für jeden Test gibt es ein WT mit WTL, der alle Testaktivitäten, einschließlich der Zusammenarbeit mit dem TI/RT-Anbieter und mögliche Treffen mit Behörden, koordiniert.

Der TI-Anbieter stellt dem Unternehmen Bedrohungsinformationen in Form eines TTI Berichts zur Verfügung. TI-Anbieter sollten mehrere Informationsquellen nutzen, um eine möglichst genaue und aktuelle Bewertung zu erhalten. Der TTI-Bericht beschreibt die Bedrohungsszenarien, die vom RT-Anbieter verwendet werden können, um Angriffsszenarien für den Red Team Test zu entwickeln.

Das BT umfasst die Mitarbeiter der Einheit, die nicht Teil des WT sind. Das BT wird vollständig von der Vorbereitung und Durchführung des Tests ausgeschlossen. Während der Abschlussphase, wird das BT über die Durchführung des Tests informiert. Die relevanten und am besten geeigneten Mitglieder des BT werden bei einer Wiederholung und der Nachbearbeitung beteiligt.

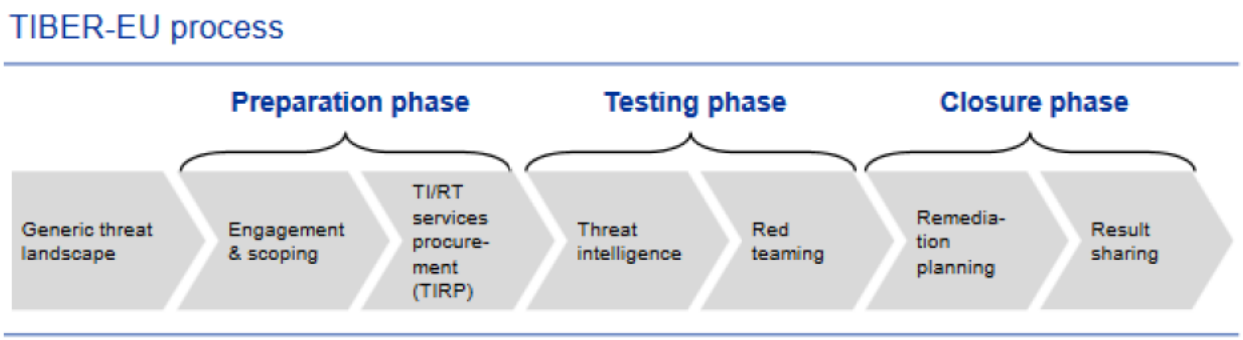
Der RT-Provider plant und führt einen TIBER-EU Test der im Umfang vereinbarten Zielsysteme und -dienste durch. Es folgt eine Überprüfung des Tests und der auftretenden Probleme, die in einen vom RT-Anbieter erstellten Red Team Testbericht münden.

Die Durchführung des TIBER-EU-Prozess ist in Phasen eingeteilt. Bevor die erste Phase beginnt, kann eine optionale Phase zur Erstellung einer Bedrohungslandschaft (engl. Genereic Threat Landscape (GTL)) vorangestellt werden. Die GTL-Phase beinhaltet eine Bewertung der Bedrohungslandschaft des nationalen Finanzsektors, in der die spezifischen Rollen der Unternehmen (z. B. Investmentbanken, Geschäftsbanken, Zahlungssysteme, zentrale Gegenparteien, Börsen usw.) umrissen werden. Hierbei werden die relevanten High-End-Bedrohungsakteure für den Sektor und die auf diese Unternehmen ausgerichteten TTPs identifiziert. Die GTL verbindet die Bedrohungsakteure und ihre TTPs mit den spezifischen Einheiten des Sektors und kann als Grundlage für die spätere Entwicklung von Angriffsszenarien dienen. Die GTL kann vom nationalen Geheimdienst nach Möglichkeit

validiert, überprüft und laufend aktualisiert werden, wenn neue Bedrohungsakteure und TTPs entstehen und ein Risiko für das Unternehmen besteht.

Der TIBER-EU Prozess ist in die Phasen Vorbereitung (engl. Preparation), Testen (engl. Testing) und Abschluss (engl. Closure) aufgeteilt (siehe Abbildung 17: TIBER-EU). Diese Phasen sind verpflichtend durchzuführen.

Abbildung 17: TIBER-EU Prozess



Die Phasen werden in folgender Tabelle beschrieben:

Tabelle 10: Phasen im TIBER-EU Prozess

Phase	Beschreibung
Vorbereitung (engl. Preparation)	Die Vorbereitung beinhaltet das Engagement, Scoping und die Auftragsvergabe. Beim Engagement wird der Test formell eingeleitet und die für die Durchführung des Tests verantwortlichen Teams gebildet. Das Scoping legt den Umfang des Tests fest, der vom Vorstand des Unternehmens bestimmt, genehmigt, bestätigt und von den zuständigen Behörden validiert wird. Zudem werden in dieser Phase die TI- und RT-Anbieter zur Durchführung des Tests beauftragt.
Testen (engl. Testing)	Zum Testen gehört das TI und RT. Während dieser Phase erstellt der beauftragte TI-Anbieter einen TTI-Report über das Unternehmen, der Bedrohungsszenarien für den Test und nützliche Informationen über das Unternehmen enthält. Hier arbeitet der TI-Anbieter eng mit dem RT-Anbieter zusammen. Falls vorhanden, wird die GTL als Basis eingesetzt. Der TTI-Bericht wird vom RT-Anbieter verwendet, um Angriffsszenarien zu entwickeln und einen Red Team Test durchzuführen, der den kritischen Funktionen der Organisation zugrunde liegt.
Abschluss (engl. Closure)	Der Abschluss besteht aus der Behebungsplanung und dem Ergebnisbericht. Während dieser Phase erstellt der RT-Anbieter einen Red Team Test Report (RTT Report), der Details über den Ansatz bei der Prüfung und die Ergebnisse und Beobachtungen aus dem Test enthält. Gegebenenfalls wird der Bericht Empfehlungen zu Verbesserungsbereichen in Bezug auf technische Kontrollen, Richtlinien und Verfahren sowie Aufklärung und Sensibilisierung enthalten. Die Hauptakteure sind nun über den Test informiert und sollten die ausgeführten Szenarien wiederholen und die während des

Phase	Beschreibung
	Tests aufgedeckten Probleme diskutieren. Die betroffene Stelle muss anschließend unter Berücksichtigung der Ergebnisse und in Absprache mit der Aufsicht einen Behebungsplan vereinbaren und abschließen. Der Ablauf des Tests wird geprüft und diskutiert und die wichtigsten Ergebnisse werden mit anderen zuständigen Behörden ausgetauscht. Die Genehmigung zum Abschluss der Prüfung sollte von den zuständigen Behörden eingeholt werden, sobald der Behebungsplan vereinbart wurde.

Der TIBER-EU-Test birgt aufgrund der Kritikalität der Zielsysteme, der Personen und der an den Tests beteiligten Prozessen Risikoelemente für alle Beteiligten. Die Möglichkeit, einen Denial-of-Service Vorfall, einen unerwarteten Systemabsturz, Schäden an kritischen Live-Produktivsystemen oder den Verlust, die Änderung oder Offenlegung von Daten zu verursachen, unterstreicht die Notwendigkeit eines Risikomanagements. Das Unternehmen ist verantwortlich für die Implementierung geeigneter Maßnahmen, Prozesse und Verfahren, um sicherzustellen, dass die Risiken im Test gemäß Best-Practices identifiziert, analysiert und gemindert werden. Bereits vor der Prüfung sollte eine Risikobewertung durchgeführt werden und während der gesamten Durchführung des TIBER-EU-Tests sicherstellen, dass es die mit dem Test verbundenen Risiken angemessen berücksichtigt.

Damit in einem Land ein TIBER-Test durchgeführt werden kann, muss sich zuerst die zuständigen Behörden (Zentralbank, Bankaufsicht, etc.) zusammenfinden und eine eigene TIBER-Implementierung umsetzen. Dies ist zum Beispiel in den Niederlanden und in Belgien schon geschehen. In Deutschland gibt es noch keine eigene Umsetzung von TIBER-DE, d. h. ein TIBER-EU Test ist in Deutschland nach dem Framework noch nicht umsetzbar. Nach Aussage des BSI Präsident Arne Schönbohm wird bis zur Umsetzung von TIBER-DE Framework noch etwas Zeit ins Land gehen. Ab wann ein Red Team Test nach dem TIBER Framework in Deutschland möglich ist, ist bei der Durchführung der Masterarbeit nicht bekannt.[88] Das TIBER-EU richtet sich an Unternehmen, die für das Funktionieren des Finanzsektors entscheidend sind (z. B. Banken, Börsen, Ratingagenturen, Versicherungsunternehmen, ...), kann aber auch von anderen Sektoren angewandt werden.

2.10.6 Fazit

Im SANS Whitepaper wurde bereits 2013 die Notwendigkeit von Red Teaming beschrieben. Mit Red Teaming sollen laut dem Whitepaper möglichst alle Schwachstellen identifiziert werden. Der Sicherheitstest zielt vor allem auf technische Aspekte der Netzwerk- und Systemebene ab. Dabei soll ein mehrstufiger Ansatz gewählt werden, d. h. mehrere Arten von Angriffen durchgeführt und auf unterschiedlichen Ebenen in der Defense-in-Depth geprüft werden, sodass die Sicherheit einer Organisation bewertet werden kann. Dabei wird auch verdeutlicht, das Red Teaming keine allgemeine Informationssicherheit bietet, sondern ein kontinuierlich verbessertes ISMS notwendig ist.

[88] Vgl. *Beermann, J./Schönbohm, A.*, Hacken für die gute Sache – Cybersicherheit auf dem Prüfstand, 2018.

2014 hat Microsoft ein Whitepaper zu Red Teaming in der Microsoft Enterprise Cloud veröffentlicht, in dem ein Prozess zur Verbesserung der Widerstandsfähigkeit gegen Angriffe von Microsoft beschrieben wird. Bestandteil davon ist Red Teaming. Das Red Teaming wird durch weitere Maßnahmen wie eines Wargaming-Workshops ergänzt.

Im Jahre 2015 wird von NIST der Red & Blue Team Ansatz beschrieben. Dort wird beschrieben, dass mit Red Teaming die Angriffs- oder Exploit-Fähigkeiten eines potenziellen Angreifers angewendet werden, mit dem Ziel die Informationssicherheit im Unternehmen zu verbessern, indem die Auswirkungen erfolgreicher Angriffe aufgezeigt werden.

Die Organisation CREST hat 2016 ein Framework veröffentlicht, in dem unter anderem Sicherheitstests beschrieben sind, die auf Bedrohungsinformationen basieren. Mit kontrollierten, maßgeschneiderten und intelligent gesteuerten Tests wird das Verhalten von Bedrohungsakteuren repliziert. Die CBEST-Dienstleister müssen sich an bestimmte Verhaltenskodizes halten.

Seit 2018 gibt es das TIBER-EU Framework der EZB. In diesem wird das Threat Intelligence-based Ethical Red Teaming dargestellt. In diesem werden die unterschiedlichen Teams und der Prozess von Red Teaming beschrieben. Das Framework dient als Basis, um TIBER zu implementieren. Um TIBER in Deutschland implementieren zu können, fehlt noch ein Rahmenwerk für Deutschland.

CREST und das TIBER-EU beschreiben beide Red Teaming das auf Bedrohungsinformationen basiert. Von SANS, Microsoft und NIST wird dagegen ein genereller Ansatz von Red Teaming beschrieben. Bei Microsoft ist Red Teaming ein Teil von einem Prozess, der durchlaufen wird, um die Widerstandsfähigkeit gegen Cyber-Angriffe zu verbessern. Die Dokumente der EZB und CREST geben umfangreiche Informationen auf dessen Basis Red Teaming durchgeführt werden kann. CREST und TIBER sind grundsätzlich auf die Finanzbranche ausgelegt, können aber auch auf andere Branchen übertragen werden.

3 Rechtliche Rahmenbedingungen

> Bei den meisten Unternehmen dürfte ein gezielter Cyberangriff den Fortbestand gefährden. Der Gesetzgeber hat das ebenfalls erkannt und daher beispielsweise in § 91 Abs. 2 Aktiengesetz bestimmt: „Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden." Die gleiche Verpflichtung trifft den Geschäftsführer einer GmbH. Ein Red Team Assessment kann hier helfen, die „wunden Punkte" eines Unternehmens zu finden, und Maßnahmen gegen einen den Fortbestand des Unternehmens gefährdenden Cyberangriff zu erkennen, planen und ergreifen. Diese Verpflichtung darf die Unternehmensleitung keinesfalls auf die leichte Schulter nehmen, denn sollte sie keine geeigneten Präventionsmaßnahmen treffen, haftet sie persönlich mit ihrem eigenen Vermögen (z. B. gem. § 93 Abs. 1 Aktiengesetz). Ist in einer Aktiengesellschaft ein IT-Vorstand bestimmt, in dessen Aufgabenkreis die Cybersicherheit typischerweise fällt, haftet dieser allein.[89]

Grundsätzlich sind die rechtlichen Rahmenbedingungen vergleichbar mit denen eines Penetrationstests. Daher wurde auf Grundlage des Artikels „*Penetrationstest*" von der Rechtsanwaltskanzlei Wilde Beuger Solmecke folgende Tabelle erstellt (siehe Tabelle 11: Übersicht der relevanten Gesetze). Diese soll einen Überblick über die relevanten Gesetze geben. Die genannten Gesetze haben keinen Anspruch auf Vollständigkeit, da sich jene nach Branche und Land unterscheiden können. Zudem hat der Autor dieser Masterarbeit keinen juristischen Hintergrund.

Tabelle 11: Übersicht der relevanten Gesetze[90/91]

Gesetz	Bezeichnung	Beschreibung
§202a StGB	**Ausspähen von Daten**	Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit einer Freiheitsstrafe von bis zu drei Jahren oder einer Geldstrafe bestraft.
§202b StGB	**Abfangen von Daten**	Mit einer Freiheitsstrafe bis zu zwei Jahre oder Geldstrafe wird bestraft, wer sich unbefugt nicht für ihn bestimmte Daten verschafft, also Daten ohne Überwindung eines Zugangshindernisses etwa während eines Übertragungsvorgangs abfängt.
§ 202c StGB	**Vorbereiten des Ausspähens und**	Der Erwerb, die Herstellung und der Einsatz von sog. Hackersoftware ist strafbar, wegen des Vorbereitens des Ausspähens und

[89] *IX-REDAKTION*, iX Kompakt (2019) IT-Sicherheit., S. 101.
[90] Vgl *Solmecke, C.*, Penetrationstest.
[91] Vgl. *Thode, J.*, Arbeitgeber ist kein Diensteanbieter im Sinne des TKG wenn die private Internetnutzung erlaubt ist, 2016.

Gesetz	Bezeichnung	Beschreibung
	Abfangens von Daten (Hackerparagraph)	Abfangens von Daten. Darunter werden auch das Beschaffen und Verbreiten von Passwörtern oder sonstigen Sicherheitscodes sanktioniert. Auf diese Straftat steht eine Freiheitsstrafe bis zu zwei Jahren oder eine Geldstrafe. Der bloße Besitz eines Computerprogramms, das für die Begehung von Straftaten geeignet ist, genügt nicht, um eine Strafbarkeit zu begründen, denn: faslls solche Programme zu erlaubten Tätigkeiten genutzt werden, fehlt der für die Strafbarkeit notwendige Vorsatz. Aus diesem Grund ist ein Penetrationstest nicht strafbar, wenn die Software im Rahmen des vereinbarten Tests eingesetzt wird.
§303a StGB	**Datenveränderung**	Strafbar ist es, durch einen Angriff rechtswidrig Daten zu löschen, zu unterdrücken, unbrauchbar zu machen oder zu verändert. Bei dieser Straftat wird eine Freiheitsstrafe von bis zu zwei Jahren oder eine Geldstrafe verhängt.
§303b StGB	**Computersabotage**	Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er rechtswidrig Daten löscht, unterdrückt, unbrauchbar macht oder verändert, Daten in der Absicht, einem anderen Nachteil zuzufügen, eingibt, übermittelt oder eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert wird mit einer Freiheitsstrafe von drei und in schweren Fällen sogar bis zu 10 Jahren oder einer Geldstrafe bestraft. Unter diesem Paragrafen werden unter anderem DDoS-Attacken sanktioniert.
§ 17 UWG	**Verrat von Geschäfts- und Betriebsgeheimnissen**	Wenn ein Angreifer an Betriebs- oder Geschäftsgeheimnisse kommt, kann eine Strafbarkeit gegen unlauteren Wettbewerb in Betracht kommen, wenn dabei aus Eigennutz oder mit Schädigungsabsicht gehandelt wurde.
§ 44 BDSG	**Klagen gegen den Verantwortlichen oder Auftragsverarbeiter**	Wer aus Bereicherungs- oder Schädigungsabsicht in Bezug auf personenbezogene Daten handelt kann mit einer Freiheitstrafe von bis zu zwei Jahren sanktioniert werden.

Gesetz	Bezeichnung	Beschreibung
§ 106 UrhG	**Unerlaubte Verwertung urheberrechtlich geschützter Werke**	Wer urheberrechtlich geschützte Informationen stiehlt und verwertet, kann nach dem Urheberrechtsgesetzt mit einer Freiheitsstrafe von bis zu drei Jahren bestraft werden.
§3/ §88 TKG	**Diensteanbieter / Fernmeldegeheimnis**	Jeder, der Telekommunikationsdienste (z. B. E-Mail, Internet) erbringt oder an der Erbringung solcher Dienste mitwirkt ist ein Diensteanbieter. Man zählt nicht unter den Diensteanbieter, wenn die private Nutzung erlaubt ist. Wenn das Unternehmen unter das TKG fällt, müssen alle Benutzer zustimmen oder die geforderten Geheimhaltungspflichten (§89 TKG) eingehalten werden. Dies sollte im Idealfall durch eine Betriebsvereinbarung geregelt sein.
§89/ § 90 TKG	**Abhörverbot, Geheimhaltungspflichten / Missbrauch von Sendeanlagen**	Wenn ein Unternehmen unter das TKG fällt, gibt es ein Verbot, Daten im Netzwerk abzuhören. Hier ist - falls nicht anders geregelt - eine Einwilligung des Personenkreises notwendig.
§ 148 TKG	**Strafvorschriften**	Das Abhören von Nachrichten ist ein Verstoß gegen das Fernmeldegeheimnis (TKG) mit einer Freiheitsstrafe von bis zu zwei Jahren oder einer Geldstrafe strafbar.
§ 87 BetrVG	**Mittbestimmungsrechte Betriebsrat**	Wenn keine andere gesetzliche oder tarifliche Regelung besteht, hat der Betriebsrat bei der Einführung und Anwendung von technischen Einrichtungen, die bestimmt sind das Verhalten oder die Leistung der Arbeitnehmer zu überwachen, Mitspracherechte. Dies muss ggf. berücksichtigt werden.

Wenn ein Auftraggeber ein Red Teaming bei einem Dienstleister beauftragt, muss ein Dienstleistungsvertrag mit den Inhalten wie der Vorgehensweise, den Zielen und dem Testzeitraum abgeschlossen werden.

Damit eine strafrechtliche Verfolgung ausgeschlossen wird, sollte zusätzlich ein Freigabeformular bzw. eine explizite Einverständniserklärung aller Beteiligten mit dem Testzeitraum, dem Ziel (z. B. IP-Netz-/ -Adresse/ URL), der Quelle, von der aus die Angriffe durchgeführt werden (in der Regel die IP-Adressen) und dem Ansprechpartner im Testverlauf seitens des Kunden unterschrieben werden. Dadurch bestätigt der Kunde, dass er über die Risiken bei der Durchführung in Kenntnis gesetzt worden ist. Ein solches Dokument wird im Fachjargon als „Du kommst aus dem Gefängnis frei“ (engl. Get out of Jail)-Karte bezeichnet. Wichtig zu beachten ist, dass sich der Tester strafbar macht, falls er nicht

mit dem Einverständnis des Unternehmens oder außerhalb des vereinbarten Rahmens agiert.

Ebenfalls wichtig ist, das Projekt, falls vorhanden, mit dem Betriebsrat abzusprechen und genehmigen zu lassen. Auch einen Geheimhaltungsvertrag (engl. Non-disclosure Agreement (NDA)) mit dem Dienstleister abzuschließen ist übliche Praxis.

> Analog zum generellen Angriff auf Systeme gilt auch im Zusammenhang mit Malware oder Trojanern, dass sie nur auf Endgeräten platziert werden, die ausschließlichen dem Unternehmen gehören und von ihm genutzt werden. Sollte der Tester darüber hinaus Endgeräte infizieren, die im Privateigentum und in privater Nutzung eines Mitarbeiters stehen, hätte er hierzu keine rechtliche Befugnis. Er würde sich strafbar machen und sähe sich wie das Unternehmen Schadensersatzansprüchen der Betroffenen ausgesetzt.[92]

Privatpersonen haben die Möglichkeiten sich bezüglich dem Datenschutzrecht an den zuständigen Landesdatenschutzbeauftragten bzw. die Aufsichtsbehörde zu wenden und sich kostenlos beraten zu lassen. Dies wurde im Rahmen dieser Arbeit genutzt und folgende Fragestellung formuliert.

Frage

„Im Rahmen von einem Red Teaming kann es dazu kommen, dass Datenschutzrechte verletzt werden, indem bspw. Zugriff auf ein fremdes E-Mail-Postfach von einem Mitarbeiter möglich ist. Wie sollten Dienstleister und Auftraggeber damit umgehen? Reicht es aus, dass ein Dienstleistungsvertrag besteht, der die Erlaubnis erteilt Angriffe/ Sicherheitstests durchzuführen, oder ist eine Einwilligungserklärung für Datenschutz bei einem solchen Test erforderlich? Falls eine zusätzliche Einwilligungserklärung notwendig ist, was sollte darin geregelt werden? Wie ist die Rechtslage laut DSGV?“

Antwort

„Mit einer solchen Maßnahme ist zunächst das Risiko der Strafbarkeit verbunden (z. B. §§ 202a ff, 303a StGB). Man sollte also mit der zu prüfenden Stelle den Test hinreichend genau vereinbart haben. Soweit Daten Dritter betroffen sein können (sowohl personenbezogene Daten, was das Datenschutzrecht interessiert, als auch z. B. Geschäftsgeheimnisse, vgl. GeschGehG), ist sicherzustellen, dass es legal ist, als "Angreifer" auf diese Daten zugreifen zu können bzw. zuzugreifen. Hier könnte sich z. B. ein Auftragsverarbeitungsvertrag (Art. 28 DS-GVO) anbieten. Es können sich weitere Fragen ergeben, je nachdem, wer prüft (z. B. eine Datenschutz-Aufsichtsbehörde, vgl. dazu Krischker, ZD 2015, 464), wer geprüft wird (z. B. eine Sozialbehörde - vgl. § 80 SGB X) und ob sich die zu prüfenden Gerätschaften überhaupt im Inland befinden (zu völkerrechtlichen Aspekten z. B. Ziebarth, Online-Durchsuchung, 2013). Möglicherweise besteht sogar eine Pflicht für derartige Überprüfungen, vgl. Mantz, in: Sydow, DS-GVO, 2. Aufl., Art. 32 Rn. 20 m.w.N.“

[92] *IX-REDAKTION*, iX Kompakt (2019) IT-Sicherheit, S.101.

Aus der Antwort eines Mitarbeiters des Landesdatenschutzbeauftragten kann entnommen werden, dass es sich anbietet einen Auftragsverarbeitungsvertrag abzuschließen, falls Daten Dritter, z. B. personenbezogene Daten oder Geschäftsgeheimnisse betroffen sind. Zudem müssen weitere Fragen geklärt sein, je nachdem wer prüft, wer geprüft wird und in welchem Land sich das zu prüfende Gerät befindet. Generell gilt, dass für alles was von einem Red Team getan wird ein Einverständnis des Auftraggebers vorliegen muss. Es ist auch zu empfehlen sich ggf. oder im Zweifel juristische Beratung einzuholen, um eine juristisch eindeutig vertretbare Durchführung zu gewährleisten.

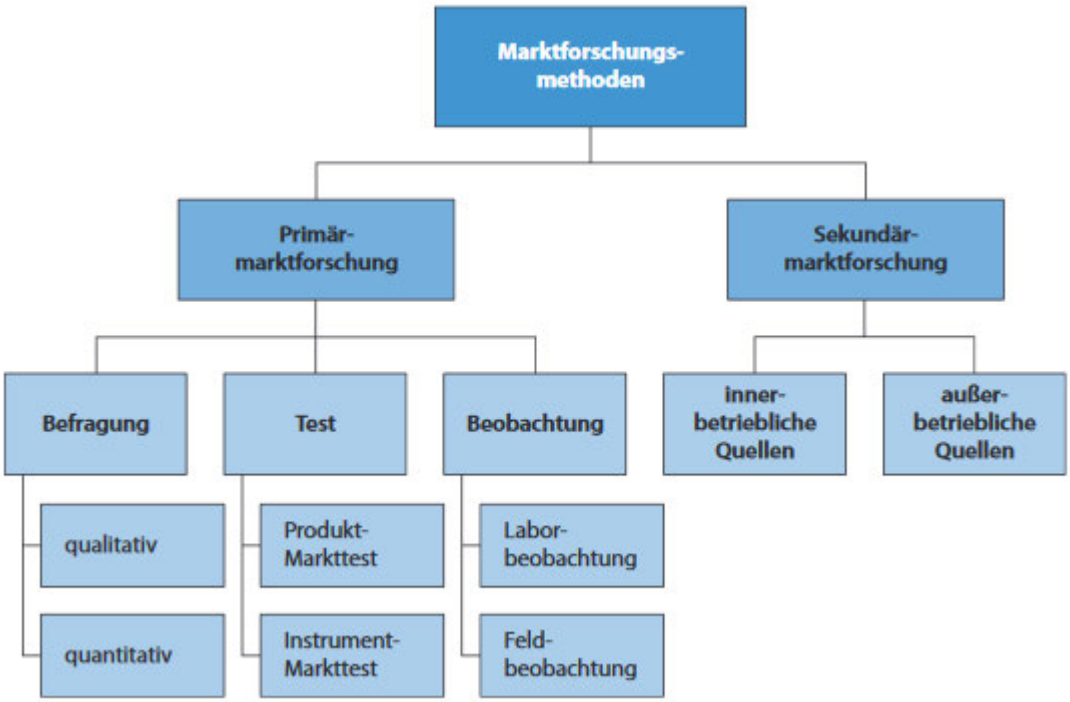
4 Marktforschung

> Die Marktforschung kann definiert werden als systematische auf wissenschaftlichen Methoden beruhende Gewinnung und Auswertung von Informationen über die Elemente und Entwicklung des Marktes unter Berücksichtigung der Umweltbedingungen. Ziel ist die Bereitstellung von objektiven Informationen und Analysen, die als Grundlage für die Planung, Entscheidung, Aufgabenübertragung und Kontrolle von Marketingmaßnahmen dienen.[93]

Die Marktforschung kommt aus der Betriebswirtschaftslehre, genauer aus deren Marketingbereich. Im Marketing wird die Marktforschung genutzt, um auf dieser Grundlage die Marketingstrategie bzw. geeignete Marketingmaßnahmen abzuleiten und auszuwählen. Mit einer Marktanalyse kann ein gegenwärtiges Bild über die Struktur und Größe des Marktes abgegeben werden. Eine Marktanalyse ist eine statische Analyse. Die Art der Informationsgewinnung wird auch in Primär- (engl. field research) und Sekundärmarktforschung (engl. desk research) unterteilt. Mit der Primärmarktforschung werden Informationen für eine Fragestellung mit einer eigens dafür konzipierten Erhebung gewonnen. Bei der Sekundärforschung wird auf vorhandene Informationen zurückgegriffen. Einen Überblick über die Marktforschungsmethoden kann der folgenden Abbildung entnommen werden.[94]

[93] *Thommen, J.-P./Achleitner, A.-K./Gilbert, D. U.*, Allgemeine Betriebswirtschaftslehre, 2017, S. 70.
[94] Vgl. *Thommen, J.-P./Achleitner, A.-K./Gilbert, D. U.*, Allgemeine Betriebswirtschaftslehre, 2017, S. 70-71.

Abbildung 18: Überblick Marktforschungsmethoden[95]



4.1 Sekundärmarktforschung

Diese Arbeit beginnt mit der Sekundärmarktforschung, d. h. auf Grundlage außerbetrieblicher Quellen – dem Internet – wird eine Marktanalyse durchgeführt. In der Marktanalyse geht es darum, die Anbieter ausfindig zu machen, die Red Teaming als Dienstleistung anbieten. Für die Onlinesuche wurde searx.me verwendet. Mit der Suche können die Ergebnisse mehrere Suchmaschinen aggregieren werden. Die Suchmaschine speichert keine Informationen über den Benutzer.[96] Zur Suche wurden die zwei meistgenutzten Suchmaschinen Google und Bing ausgewählt.[97] Als Suchbegriffe wurde „Red Teaming", „Red Team Test" und „Red Team Assessment" verwendet. Über die Anbieter wurden folgende Informationen gespeichert:

- Firmennamen
- Geographische Lage

Zusätzlich wurden per LinkedIn folgende Informationen zu den Unternehmen ergänzt:

- Branche
- Mitarbeiteranzahl
- Hauptsitz
- Gründungsjahr

[95]Vgl. *Thommen, J.-P./Achleitner, A.-K./Gilbert, D. U.*, Allgemeine Betriebswirtschaftslehre, 2017, S. 71.
[96]Vgl. *searx.me*, About searx.
[97] Vgl. *Rabe, L.*, Marktanteile der meistgenutzten Suchmaschinen weltweit bis Mai 2019, 2019.

- Spezialgebiete

Die Informationen bei den Unternehmen ohne LinkedIn-Webseite wurden manuell recherchiert. Die Ergebnisse der Sekundärmarktforschung dienen als Übersicht über den Markt und als Grundlage für die Primärforschung (siehe 4.2 Primärmarktforschung).

4.1.1 Auswertung

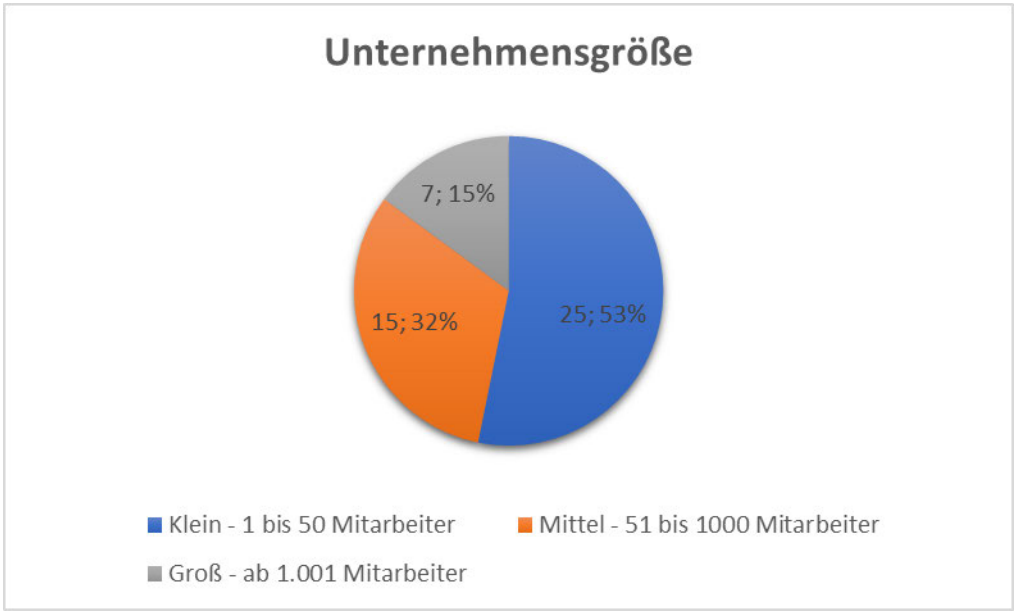
Im Anhang Anlage 1 befindet sich die Tabelle mit den recherchierten Dienstleistern. Zu den Dienstleistern wurden weitere ergänzt, die in den Suchergebnissen nicht aufgetaucht sind, bei denen aber bekannt ist, dass das Unternehmen Red Teaming als Dienstleistung anbietet.

Bei der Marktanalyse wurden insgesamt 47 Unternehmen gefunden. Die Unternehmen wurden in drei Größenklassen eingeteilt:

- Klein – 1 bis 50 Mitarbeiter
- Mittel – 51 bis 1000 Mitarbeiter
- Groß – ab 1.001 Mitarbeiter

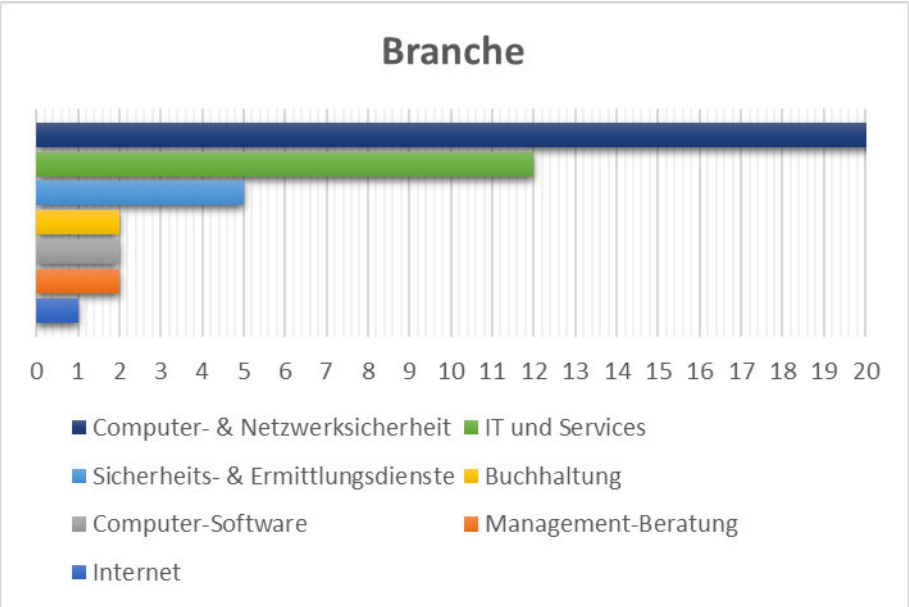
53% der Dienstleister haben eine Mitarbeiteranzahl zwischen einem und fünfzig Mitarbeitern. 31% haben eine Mitarbeiteranzahl zwischen 51 bis 1.000 und 16% sind größer (siehe Abbildung 19: Unternehmensgröße).

Abbildung 19: Unternehmensgröße



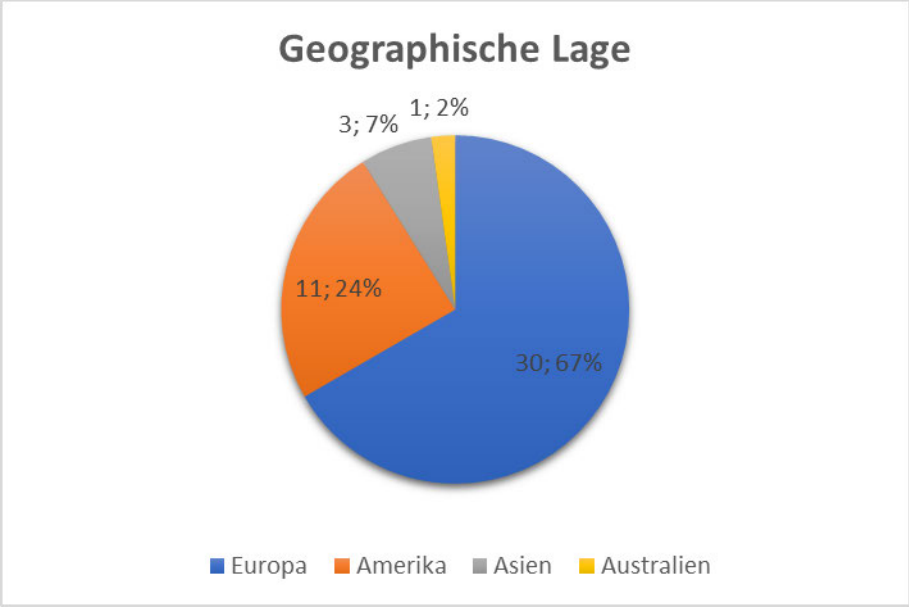
Von den 47 Unternehmen geben 25 auf LinkedIn an, in der Branche *Computer- und Netzwerksicherheit,* 12 Unternehmen in *IT und Service* und fünf sind in *Sicherheit und Ermittlungsdienste* tätig zu sein. Die restlichen Unternehmen geben die Branchen *Buchhaltung*, *Management-Beratung* und *Computer-Software* an (siehe Abbildung 20: Branche).

Abbildung 20: Branche



Im folgenden Diagramm wurde die geographische Lage der Dienstleister ausgewertet. Der Kontinent wurde nach dem Hauptsitz des Unternehmens zugeordnet. Der Großteil der Dienstleister hat den Hauptsitz in Europa mit 67%. 24% der Dienstleister kommen aus Amerika (weitere Informationen siehe Abbildung 21: Geographische Lage). Die weiteren 9% teilen sich in Asien und Australien auf. Hierbei ist zu beachten, dass eine Sprachbarriere mit Asien besteht und sehr wahrscheinlich aus diesem Grund Dienstleister nicht gefunden werden.

Abbildung 21: Geographische Lage



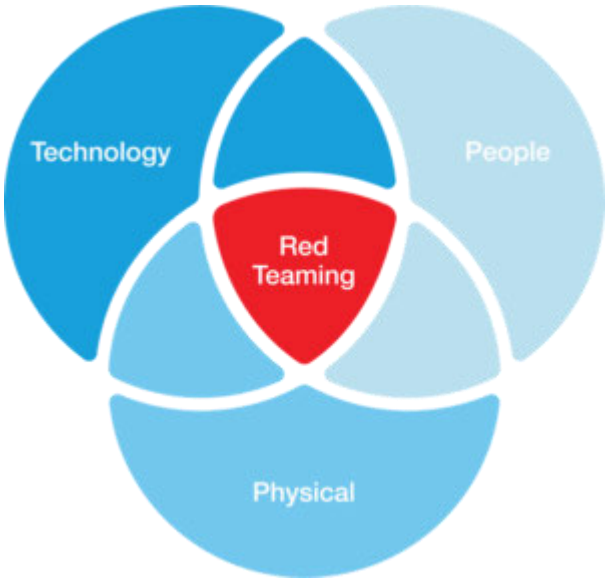
Als für diese Masterarbeit relevant wurden die 25 Unternehmen aus dem DACH-Raum ausgewählt, allesamt mit Sitz in Deutschland, Österreich oder der Schweiz.

4.1.2 Analyse Webseiteninformationen

Zur Vorbereitung der Interviews wurde das Angebot, das auf der Webseite der Dienstleister ausgeschrieben ist, betrachtet. Die Informationen zum Thema Red Teaming, die von den Dienstleistern veröffentlich wurden, sind sehr unterschiedlich. Es gibt Dienstleister, die keine oder nur wenig Informationen preisgeben, und welche, die ausführlichen Informationen oder ein Whitepaper darüber veröffentlichen.

Eine Gemeinsamkeit, die aus den Webseiten hervorgeht, ist, dass ein Red Teaming Projekt aus Tests der Komponenten Technologie, Personen oder Physisch bestehen kann. Dies wird in der folgenden Abbildung illustriert.

Abbildung 22: Red Teaming Komponenten[98]



Auf den Webseiten wird häufig genannt, dass der Angriff aus Sicht eines Angreifers ist. Mit Red Teaming sollen ein realer Angriff simuliert und TTPs von Angreifern nachgeahmt werden. Dabei werden realistische Szenarien und Bedrohungen verwendet, sowie komplexe Angriffssimulationen durchgeführt. Red Teaming wird als ein zielgerichteter Eindringversuch bezeichnet.

Um ein Red Teaming durchzuführen, wird von den Dienstleistern ein festgelegtes Ziel ausgewählt, das erreicht werden muss. Ein Ziel kann bspw. sein, an sensible Daten des Unternehmens zu kommen. Das Hauptziel von Red Teaming ist es, die Resilienz einer Organisation gegenüber bekannten und relevanten Bedrohungsakteuren zu bewerten. Mit dem Test soll das Blue Team bzw. die Erkennungs- und Reaktionszeit des Unternehmens verbessert werden. Zudem wird die Belegschaft darauf vorbereitet, auf einen Angriff ohne Vorankündigung zu reagieren. Außerdem sollen Sicherheitskontrollen geprüft, Incident Response Pläne getestet und das Unternehmen auf einen Sicherheitsvorfall vorbereitet werden, so die Aussage vieler Dienstleister. Auch das Sicherheitsbewusstsein für einen

[98] *RedTeam Security*, Full Force Red Teaming.

Sicherheitsverstoß soll verbessert werden. Als Scope des Tests wird von vielen ein ganzheitlicher Ansatz beschrieben. Bei manchen Anbietern werden bestimmte Angriffsszenarien festgelegt oder der effizienteste und effektivste Weg gesucht und ausgenutzt.

Red Teaming wird sowohl im Black-Box als auch im Gray-Box-Ansatz durchgeführt. Beim Gray-Box-Ansatz werden gewisse Informationen über die Systemumgebung ausgetauscht, um die Effizienz zu steigern. Hierbei werden von manchen Unternehmen in Abstimmung mit dem Kunden Ziele definiert. Andere Unternehmen sehen bei Red Teaming eine freie Wahl der Ziele und Mittel.

Der Ergebnisbericht soll dabei helfen, komplexe Sicherheitsschwachstellen zu beheben, das Sicherheitsbudget optimal zu nutzen und Sicherheitsmaßnahmen davon abzuleiten. Der Abschlussbericht kann durch Workshops und Training mit dem Blue Team oder Security Awareness Schulungen ergänzt werden.

Red Teaming wird für Unternehmen empfohlen die bereits zahlreiche Sicherheitsmechanismen und ein Blue Team etabliert haben. Viele Dienstleister bieten an, ein Sparringspartner für das Blue Team zu sein und mit diesem zusammenzuarbeiten.

4.1.3 Fazit

Die Sekundärmarktforschung hat ergeben, dass die meisten Unternehmen, die Red Teaming als Dienstleistung anbieten, klein sind und der Großteil in der Branche Computer- und Netzwerksicherheit tätig ist, d. h. auf das Themengebiet spezialisiert. Die meisten Unternehmen sind in Europa und Amerika angesiedelt. Auf den Webseiten der Dienstleister werden teilweise keine oder nur wenig Informationen veröffentlicht. Andere bieten umfangreiche Informationen an. Das Angebot unterscheidet sich je nach Dienstleister. Als die Gemeinsamkeit kann gesehen werden, das Red Teaming in Sicherheitstests physische, technische und menschliche Komponenten betreffen kann. Durch unangekündigte nachgestellte reale Angriffe soll die Widerstandsfähigkeit der Unternehmen verbessert werden.

4.2 Primärmarktforschung

Um Detailwissen und praktische Erfahrungen zu machen, wird in der Primärforschung eine Befragung durchgeführt. Darunter versteht man ein planmäßiges Vorgehen mit der Zielsetzung, eine Person mit gezielten Fragen zur Angabe der gewünschten Informationen zu bewegen. Eine quantitative Umfrage wird durchgeführt, wenn eine relativ große Anzahl von Befragten vorliegt. Die Anzahl von IT-Sicherheitsdienstleistern ist als gering anzusehen. Aus diesem Grund wird eine qualitative Umfrage durchgeführt. In einer qualitativen Umfrage geht es in erster Linie um eine Motiv- und Meinungserhebung. Die grundlegende Einstellung der Befragten und deren Unternehmen wird dabei erforscht. Anhand von Einzelgesprächen wird ein strukturiertes und geleitetes Interview durchgeführt. Hierbei wird ein Fragenkatalog, als Leitfaden zur Gestaltung des Interviews erstellt, um eine gewisse

Grundlinie vorzugeben. Die Interviews sind eine Kombination aus schriftlicher Befragung und telefonischem Gespräch. Der Fragenkatalog wird der Auskunftsperson zugeschickt, damit er sich ggf. darauf vorbereiten und die benötigten Informationen zurechtlegen kann. Ein telefonisches Interview bietet ein höherer Detailgrad als dies im Normallfall bei einer schriftlichen Umfrage der Fall wäre.[99]

Von den 25 Unternehmen, die im DACH-Raum Red Teaming als Dienstleistung anbieten, wurden Mitarbeiter angefragt, die bereits praktische Erfahrung mit Red Teaming gesammelt haben. Zur Vorbereitung auf die Interviews wurde ein Fragenkatalog entwickelt. Um Detailwissen und praktische Beispiele zu erfahren, wurden thematische Zwischenfragen gestellt. Der Fragenkatalog wurde in folgende Kategorien eingeteilt:

- Beschreibung
- Ziel
- Ablauf/ Prozess
- Technik/ Werkzeug
- Unterschiede
- Gemeinsamkeiten
- Vorteile
- Nachteile
- Risiken
- Sonstiges

Pro Interview wurde ein digitales Protokoll erstellt. Anschließend wurden die Antworten in ein Dokument zusammengefasst und neu strukturiert, um die Anonymität der Teilnehmer zu wahren und eine bessere Übersichtlichkeit zu gewährleisten. Es wurde zudem versucht, bereits Cluster zu den Antworten zu bilden. Die einzelnen Stichpunkte können zu einem oder mehreren Personen gehören. Ziel war es, ein allgemeines Bild über Red Teaming herauszubekommen, und nicht etwa einzelne Dienstleister zu vergleichen.

4.2.1 Fragenkatalog Dienstleister

Die befragten Dienstleister hatten einen Sitz in DACH-Raum. Insgesamt wurden 12 Mitarbeiter von 11 unterschiedlichen Dienstleistern befragt. Bei den Interviews wurde vereinzelt auch aus Erfahrungen von mehreren Dienstleistern berichtet. Weil die meisten auf Red Teaming spezialisiert sind, lag der Fokus in den Gesprächen eher auf den Schwerpunkten Red Teaming und Penetrationstests anstatt auf Audits. Die Zusammenfassung der Interview-Protokolle sind im Anhang Anlage 2. In diesem Kapitel werden die Inhalte aus den Interviews unreflektiert wiedergegeben.

4.2.1.1 Beschreibung – Was ist Red Teaming bzw. ein Red Team Assessment?

In der Kategorie Beschreibung ging es darum, zu klären, was Red Teaming ist, um herauszufinden, was der Interviewte bzw. der Dienstleister unter einem Red Teaming

[99] Vgl. *Thommen, J.-P./Achleitner, A.-K./Gilbert, D. U.*, Allgemeine Betriebswirtschaftslehre, 2017, S. 73-74.

versteht. Bei den Beschreibungen zum Red Teaming konnten folgende Gemeinsamkeiten herausgearbeitet werden:

- bei Red Teaming sollen möglichst reale Angriffe, aus Sicht eines Angreifers oder einer Angreifer-Gruppe simuliert werden
- beim Test können sowohl technische, physische und menschliche Schwachstellen ausgenutzt werden
- In Abstimmung zwischen dem Auftraggeber und dem Red Team wird ein Ziel spezifiziert, das durch einen Eindringungsversuch ins Unternehmen erreicht werden soll.
- Das Red Team besteht aus mehreren Testern, die unterschiedliche Expertisen in bestimmten Bereichen haben. Bei den meisten haben sich zwei Tester etabliert und bei Bedarf werden weitere Spezialisten hinzugezogen.
- In der Regel ist nur der Auftraggeber (z. B. Management, Vorstand, CISO, IT-Sicherheitsbeauftragter) über den Test informiert. Es ist ein unangekündigter Test für das Blue Team bzw. die Verteidigung.

Durch die freien Antworten der Befragten gibt es sehr unterschiedliche Antworten. Der Kunde ist „König“ und der Dienstleister richtet sich nach seinen Anforderungen und Wünschen. Die Red Teaming Dienstleistung wird somit häufig auf einen Kunden zugeschnitten. Dies erklärt, warum es sehr individuell ausgeprägt sein kann. Es konnten folgende Ausprägungen von Red Teaming festgestellt werden:

Standard vs. kein Standard
Es gibt einige Unternehmen, die sich nach einem Framework wie TIBER-EU und MITRE ATT&CK oder den Rahmenwerken von CREST richten. Andere nutzten keinen Standard. Beim Ablauf eines Angriffs wurde von mehreren Teilnehmern die Cyber Kill Chain von Lockheed Martin angesprochen.

Bedrohungsanalyse vs. keine Bedrohungsanalyse
Von Dienstleistern wurde beschrieben, dass als Grundlage von Red Teaming in Abstimmung mit dem Kunden Bedrohungen, Bedrohungsmodelle (engl. Threat Models), Angriffsszenarien und Ziele erarbeitet oder ausgewertet werden. Dazu werden Erfahrungen der Beteiligten und Berichten über APTs, Antivieren-Hersteller, Blog Posts, Hackergruppen, Incident Reports, Threat Intelligence, Security Reports und Governance Reports verwendet. Aus den definierten Angriffsszenarien kann das Red Team Angriffe festlegen und simulieren. Bei manchen Dienstleistern ist dies ein fester Bestandteil und wird als Basis für Red Teaming gesehen. Es gibt auch Dienstleister, die die Bedrohungslage nicht betrachten und die Angriffe auf Grundlage gesammelter Informationen und der vorhandenen Expertise durchführen.

Blue Team vs. kein Blue Team
In den Interviews wurde ausgesagt, dass Red Teaming nur als sinnvoll angesehen wird, wenn ein Blue Team vorhanden ist. Darunter wird in diesem Zusammenhang ein Team bezeichnet, das zur Erkennung von Angriffen zuständig ist, wie ein Security Operations

Center (SOC), Computer Emergency Response Team (CERT), Security Abteilung und Incident Response Team. Es gibt auch Dienstleister, die Projekte mit Unternehmen durchgeführt haben, die kein spezielles Team für die Erkennung von Angriffen hatten. Dabei wird häufig festgestellt, dass ein Blue Team und eine Verbesserung der Sicherheitsmaßnahmen erforderlich sind.

Szenario-basierter Test vs. Red Teaming
Wenn kein Blue Team nach der Definition der Gesprächspartner vorhanden ist, wird auch von einem Szenario-basierten Test gesprochen. In diesem wird ein vordefiniertes Angriffsszenario definiert. Das Ziel hierbei ist, herauszufinden, ob bestimmte Angriffe erfolgreich wären und welche Sicherheitsmaßnahmen notwendig sind. Eine Unterscheidung zwischen einem Szenario-basierten Test und Red Teaming wird nur vereinzeln gemacht.

Red Teaming vs. Purple Teaming
Wenn das Blue durch das Red Team unterstützt wird, wird auch von Purple Teaming gesprochen. Es gibt Dienstleister, die es für sinnvoll halten, bei einem Red Teaming das Blue Team im Rahmen des Projektes zu unterstützen.

Informiert vs. uninformiert
Ein realer Angriff wird im Normalfall nicht angekündigt. Aus diesem Grund wird bei den meisten Red Teaming Projekten das Blue Team nicht darüber informiert, sodass der Angriff nicht von einem realen Angriff unterschieden werden kann. Es gibt auch Dienstleister, die dem Blue Team und den Mitarbeitern gewisse Informationen übermitteln.

Black-Box vs. Grey-Box vs. White-Box
Red Teaming wird sowohl als Black-Box-, Grey-Box (mit gewissen Informationen), wie auch als White-Box mit vollem Zugriff auf Informationen über Systeme und Prozesse durchgeführt.

Technische Sicherheit vs. physische Sicherheit vs. Social Engineering
Bei Red Teaming gibt es Projekte bei denen der Schwerpunkt auf die technische Sicherheit, Social Engineering oder physische Sicherheit gelegt wird. Es gibt aber auch Dienstleister, die durch einen Test ein oder mehrere Bereiche abdecken wollen.

Voller Scope vs. eingeschränkter Scope
Manche sehen ein Red Teaming als ein Full Scope Tests. Vor wirklicher Angriffssimulation scheuen sich aber viele Unternehmen. Aus diesem Grund wird aus einem Red Teaming häufig ein kontrollierter, stufenweiser Test mit einem bestimmten Ziel und eingeschränktem Scope gemacht.

Freie Wahl der Angriffe vs. festgelegte Angriffe
Die Wahl der Angriffsszenarien ist ebenfalls unterschiedliche. Es gibt Unternehmen, die bei Red Teaming ein genaues Szenario z. B. einen bestimmten APT simulieren möchten. Hier sind die geplanten Angriffe genau festgelegt. Andere geben dem Red Team Freiraum bei der Wahl der Angriffe.

Viele Angriffswege vs. ein Angriffsweg
Manche Dienstleister geben an, in einem Red Teaming viele unterschiedliche Angriffswege zu testen. Andere wählen den Weg des geringsten Widerstands bzw. das offensichtliche und schwächste Glied einer Sicherheitskette. Häufig ist dies abhängig von den Anforderungen des Kunden, dem Budget und der zur Verfügung gestellten Zeit.

Die Ausprägungen werden nicht nur pro Dienstleister, sondern auch pro Kundenprojekt unterschiedlich ausgelegt. Aus den erhobenen Daten kann Red Teaming in zwei große Gruppen eingeteilt werden.

- Threat-based / APT-based Red Teaming – Bedrohungs- / Angriffssimulation (engl. Threat Emulation / Attack Modeling)
  ➔ „*Bedrohungsbasiertes*“ Red Teaming
- Red Teaming – Alternative Analysemethode (engl. alternative analysis)
  ➔ „*Informations-/wissensbasiertes*“ Red Teaming

Das bedrohungsbasierte Red Teaming, wie es auch im TIBER-EU beschrieben wird, zielt darauf ab, Angriffe im Red Teaming durchzuführen, die auf die Bedrohungslage des Auftraggebers zugeschnitten sind. Dazu wird eine Bedrohungsanalyse durchgeführt, auf dieser Basis werden Angriffsszenarien und Angriffe simuliert. Dabei werden bekannte Angriffsgruppen oder APTs nachgestellt.

Die Begrifflichkeit “*informations-/wissensbasiertes*“ Red Teaming, ist nicht in der Literatur zu finden und wurde im Rahmen der Arbeit festgelegt. Damit ist gemeint, dass die Angriffe nicht auf eine vorher durchgeführte Bedrohungsanalyse, sondern auf Grundlage von gesammelten Informationen, den Anforderungen des Auftraggebers oder der Expertise (z. B. Social Engineering oder Physical Assessment) der Tester basieren. Die Tests werden im Ermessen des Red Teams und in Abstimmung mit dem Auftraggeber festgelegt.

Der Red Team Lead von Intel Toby Kohlenberg beschreibt in seiner Präsentation „*Red Teaming probably ins’t for you*“, dass Red Teaming die zwei Funktionen „*Alternate Analysis*“ (dt. Alternative Analyse) oder „*Threat Emulation/ Attack Modeling“* (dt. Bedrohungssimulation / Angriffsmodellierung) einnehmen kann.[100] Mit dieser Aufteilung wird ungefähr die Unterscheidung gemacht, die im Rahmen der Gespräche aufgedeckt wurde.

4.2.1.2 Ziel - Was ist das Ziel von einem Red Teaming? Welche Ziele werden bei einem Red Teaming festgelegt?

Was das Ziel von Red Teaming ist und welche Ziele in den Projekten festgelegt wurden, wird in diesem Block beantwortet werden. Das am häufigsten genannte Ziel von Red Teaming ist, dass die Erkennungs- und Reaktionsfähigkeit vom Blue Team getestet, gemessen und verbessert werden soll. Dabei werden die Sicherheitsmaßnahmen, Sicherheitsmechanismen und Erkennungsmöglichkeiten, die im Unternehmen eingesetzt werden, überprüft.

[100] Vgl. *Kohlenberg, T.*, Red teaming probably isn't for you, 2017.

Übergreifend kann es als ein Sicherheitstest für die Verteidigung bezeichnet werden. Weitere Nennungen waren:

- die Security Awareness z. B. beim Einsatz von Phishing zu steigern
- herausfinden, welche Maßnahmen notwendig sind, um die IT-Sicherheit zu verbessern
- Krisendokumentation zum Umgang mit Sicherheitsvorfällen erstellen
- aufdecken, wie das Unternehmen hinsichtlich IT-Sicherheit aufgestellt ist
- das Blue Team dabei unterstützen, bestimmte Angriffe zu erkennen
- dem Kunden Angriffswege aufzeigen

Bei einem Red Teaming werden Ziele festgelegt, die vom Red Team erreicht werden sollen. Die Ziele sind je Projekt kundenindividuell und werden in Abstimmung mit dem Kunden festgelegt. Viele sprechen in diesem Zusammenhang, dass die "Kronjuwelen" des Unternehmens das Ziel sind. Damit sind in der Regel wichtige und sensible Informationen, kritische Funktionen oder Maschinen eines Unternehmens gemeint.

Im Normalfall werden die Ziele vom Unternehmen vorgegeben. Da dies nicht immer für die Ansprechpartner möglich ist, werden Vorschläge unterbreitet und die Ziele in Abstimmung mit dem Kunden festgelegt. Hierzu geht der Dienstleister in einem Gespräch in die Lage der Angreifer. Zusammen mit dem Kunden wird dann erörtert, was dem Unternehmen besonders weh tut oder was das Schlimmste wäre, was einem Unternehmen passieren könnte. Folgende Beispiele waren Ziele von Red Teaming Projekten:

- Zugriff auf ein festgelegtes System, z. B. ein SAP-System mit sensiblen Daten
- die E-Mails vom Vorstand abrufen
- an bestimmte Informationen, Daten, Benutzer und Unternehmensbereiche in einem Unternehmen kommen
- Lokale- oder Domain-Administrator-Berechtigungen erhalten
- Forschungsdaten, Konstruktionsdaten und Baupläne aus einem Unternehmen extrahieren
- Zugriff auf eine Anwendung oder Datenbank
- Maschinen in einer kritischen Infrastruktur kontrollieren, z. B. eine Produktionsanlage
- Versorgung der Patienten gefährden
- das Auslesen von Kundendaten oder Finanztransaktionen

Ein wichtiger Hinweis von einem Gesprächspartner war, dass bei einem Angriff unter Umständen kein hochprivilegierter Benutzer, wie ein Domain-Administrator, benötigt wird, sondern eine bestimmte Funktion oder Benutzer ausreichen kann, um an ein festgelegtes Ziel zu kommen. Auch kann es sein, dass das Erlangen von einem Domain-Administrator in einem Unternehmen nicht kritisch ist, da z. B. in einer gewissen Domain keine sensiblen Informationen sind.

4.2.1.3 Ablauf / Prozess – Wie läuft ein Red Teaming ab?

In dieser Fragenkategorie sollten die Gesprächspartner den Ablauf von Red Teaming beschreiben. Aus den genannten Antworten wurde die folgende Beschreibung erstellt.

Das Projekt startet mit einer Kundenanfrage. In einem ersten Telefongespräch wird überprüft, ob Red Teaming die richtige Methodik für den Kunden ist. Mehrmals wurde genannt, dass eine Anfrage für Red Teaming kam, sich der Kunde aber nach einer Beratung für ein Penetrationstest entschieden hat. Wenn sich der Kunde für ein Red Teaming entscheidet, führen die Dienstleister in der Regel einen Workshop oder ein Kick-Off-Gespräch durch, in welchem die Rahmenbedingungen, Ansprechpartner, Ziele, Meilensteine und die Vorgehensweise beschrieben werden. Manche sprechen in einem solchen Workshop auch über die Bedrohungen, Angriffsszenarien, eingesetzten Sicherheitsmaßnahmen und verwendeten Standards. Nach diesen Gesprächen wird ein Angebot erstellt, ein Vertrag abgeschlossen, und es startet die Planung des Projekts. Von manchen Marktteilnehmern wird ein sogenanntes "Playbook" mit der Vorgehensweise, den Zielen, den Meilensteinen, dem Zeitpunkt usw. erstellt.

Die Durchführung startet mit einer Aufklärungsphase. Diese wird auch Open Source Intelligence (OSINT) Phase bezeichnet, da in dieser Phase Informationen über öffentliche Quellen und soziale Medien über ein Unternehmen gesammelt werden. Durch die Informationssammlung werden Zusammenhänge, auch zu Dritten, identifiziert. Das Sammeln von Informationen wird im Fachjargon auch als Information Gathering bezeichnet. Manche schauen sich auch die relevanten Bedrohungsinformationen für ein Unternehmen an. Mit diesen Informationen werden Angriffswege gesucht und es dient als Grundlage z. B. für ein Social Engineering Angriff. Die Angriffe sind abhängig von den Angriffsszenarien die mit dem Kunden vereinbart wurden, so wird bspw. Social Engineering oder ein physischer Angriff bei manchen von vornherein ausgeschlossen. Nachdem ein Angriff festgelegt wurde, wird dieser vorbereitet. Wenn ein Angriff von außen durchgeführt wird, ist der erste Meilenstein in ein Unternehmen zu kommen, sich zu persistieren und eine Verbindung nach außen aufzubauen. Anschließend prüft das Team, ob die Rechte erweitert oder Möglichkeiten bestehen, sich im Netzwerk auszubreiten. Dabei wird versucht, möglichst leise und unauffällig zu sein, damit das Blue Team einen Angriff nicht erkennt. Teilweise werden aber auch bewusste Aktionen durchgeführt, um zu testen, ob das Blue Team diese wahrnimmt. Wenn ein Ziel frühzeitig erreicht wird, werden weitere Wege gesucht. Auch bei einer Erkennung vom Blue Team wird nach einem anderen Angriffsweg gesucht. Das Red Teaming wird als ein Hin und Her zwischen dem Red und Blue Team beschrieben. Bei manchen Projekten werden während der Testphase bereits Maßnahmen eingerichtet, sodass bestimmte Angriffe nicht mehr möglich sind. Anschließend wird von einem neuen Ausgangspunkt, bei der die Maßnahme bereits überwunden ist, gestartet. Dies wird gemacht, da es trotz Behebung der Schwachstelle in Zukunft möglich sein kann, dass eine Sicherheitsbarriere wieder durchbrochen wird, bspw. durch eine neu aufgetretene Schwachstelle. Zudem möchte man herausfinden, was von dem neuen Ausgangspunkt aus für einen Angreifer möglich wäre. Während der Durchführung des Red Teaming wird

kontinuierlich dokumentiert. Diese Dokumentation wird für den Ergebnisbericht, der beim Abschluss an den Auftraggeber übergeben wird, benötigt.

Der Abschlussbericht wird an den Auftraggeber übergeben. In den meisten Fällen erfolgt eine Ergebnispräsentation. Zum Teilnehmerkreis der Präsentation zählt in der Regel das Management oder der Vorstand, CISO und Mitarbeiter aus der Security-Abteilung. Bei manchen werden auch weitere Teile der Sicherheitskette, wie ein Applikationsverantwortlicher, dazu geholt. Im Nachgang führen viele Dienstleister Workshops mit dem Blue Team durch oder nutzen das Ergebnis für Security-Awareness-Maßnahmen. Aus einem Red Teaming fallen häufig viele Aufgaben an, die im Nachgang bearbeitet werden müssen. Hier werden zum Teil Nachtests von eingeführten Maßnahmen durchgeführt.

4.2.1.4 Technik / Werkzeuge – Welche TTPs (Tactics, Techniques and Procedures (TTPs)), Methoden und Software werden verwendet?

Um häufige Tools, Taktiken, Techniken, Prozesse und Methoden zu erfahren, wurde dieser Fragenteil erstellt. Beim Red Teaming können sowohl menschliche, technische als auch physische Schwachstellen ausgenutzt werden. Unter den Dienstleister gibt es welche, die beim Red Teaming zum Großteil versuchen, auf technischem Weg ins Unternehmen zu kommen. Bei anderen ist der Anteil an Social Engineering Angriffen oder einem physischen Angriff höher. Dies ist auch zum Teil auf die Anforderungen des Kunden zurückzuführen. Unter den befragten Dienstleister gibt es auch welche, die in bestimmten Bereichen, wie der physischen Sicherheit, keine Expertise haben und daher keine Tests in diesem Bereichen machen. Dies wird damit begründet, dass es wenige bis keine APTs gibt, die einen physikalischen Zugang erfordern.

Die Auswahl der Angriffsart ist abhängig vom Kunden, der Expertise des Dienstleisters und der zur Verfügung stehenden Zeit. So wird bspw. beschrieben, dass ein Spear-Phishing-Angriff und Physical Assessment weniger Zeit und Aufwand in Anspruch nimmt, wie dies bei einem technischen Angriff der Fall wäre.

Bei den bedrohungsbasierten Red Teaming werden die TTPs aus Grundlage der Threat Intelligence und Threat Models ausgewählt. Die TTPs bestimmen die Software, die eingesetzt wird.

Die Angriffe können auch in Kombination in zusammenhängenden Angriffen durchgeführt werden. Ein physischer Angriff wird zum Beispiel gerne mit Phishing kombiniert. Beispielsweise wird eine E-Mail an einen Empfang geschickt und dann vor Ort erfragt, ob der Anhang bzw. Link geöffnet werden kann.

Physical Assessment

Das Red Teaming kommt aus dem militärischen Bereich, daher sind physischen Angriffe durchaus übliche Praxis. Bestimmte Dienstleister gehen bei einem Full-Scope Tests immer physisch vor Ort und suchen nach Schwachstellen, um in ein Gebäude zu kommen.

Um von außen in ein Gebäude zu kommen, wird das Physical Assessment häufig mit der Social Engineering Methode Tailgating kombiniert. Dabei verkleidet sich ein Tester in eine Person, die berechtigt ist, in ein Unternehmen zu kommen (z. B. Putzpersonal). Anschließend wird versucht, die Sicherheitskontrolle (menschlich oder physisch) davon zu überzeugen oder zu umgehen, um Zutritt in ein Gebäude zu bekommen, z. B. durch nachgemachte Visitenkarten oder gefälschte Mitarbeiterausweise. Auch verschlossene Türen werden mit einem Lock-Picking-Set geöffnet. Dies wird aber laut Befragten nur selten eingesetzt und benötigt.

Technical Assessment
Viele Dienstleister versuchen hauptsächlich auf technischem Weg ins Unternehmen zu kommen. Hierzu werden die von außen erreichbaren Systeme und Dienste überprüft. Zudem wird bspw. die Shodan-Suchmaschine genutzt, um Systeme mit Schwachstellen zu identifizieren. Zu den technischen Angriffen gehört auch das Einschleusen und Verschleiern von Schadprogrammen. Beim internen Zugriff auf ein System werden Windows-Bordmittel verwendet, um die Rechte auszuweiten oder sich im Netzwerk zu verbreiten. Die technischen Angriffe sind stark individuell und abhängig von der vorgefundenen Infrastruktur.

Social Engineering
Die aktuell häufigste und erfolgreichste Art, eine Malware in ein Unternehmen einzubringen, ist ein Phishing-Angriff. Bei Red Teaming wird hauptsächlich Spear-Phishing, d. h. eine gezielte Phishing E-Mail praktiziert. Durch die im Information Gathering gesammelten Informationen werden passgenaue E-Mails zur initialen Infizierung verwendet. Des Weiteren wird Tailgating verwendet, wie unter Physical Assessment bereits beschrieben wurde.

Software / Hardware
Die verwendete Software und Hardware im Red Teaming ist abhängig von der ausgewählten Angriffsart und der vorgefundenen Infrastruktur. Es gibt daher eine große Bandbreite an Tools. Mehrmals wurde beschrieben, dass sich die Tools und Vorgehensweise von einzelnen Mitarbeitern unterscheiden können. Es kommen sowohl selbstentwickelte Software, und Skripte, als auch bekannte Frameworks wie Metasploit, Cobalt Strike und Empire zum Einsatz. Allgemein gibt eine breite Palette an Software, die beim Red Teaming verwendet werden kann. Um möglichst unbemerkt zu bleiben, kommen im Netzwerk vor allem Bordmittel und Administratortools vom Betriebssystem zum Einsatz. Teilweise werden auch Schwachstellenscanner wie Nessus, OpenVAS und nmap eingesetzt. Dies ist eher selten der Fall, da diese sehr schnell und einfach erkannt werden könnte. Aufgrund der hohen Komplexität in den unterschiedlichen Infrastrukturen sind viele manuelle Schritte notwendig und nur wenig bis gar nichts kann automatisiert werden. Zusätzlich können Hardware Hacking Tools, wie USB-Key-Logger, Rubber Ducky und Hardware zum Zugangskarten zu kopieren oder ähnliches zum Einsatz kommen. Kameras sind beim Physical Assessment zur Dokumentation nützlich.

4.2.1.5 Unterschiede – Wo liegt der Unterschied zwischen einem Red Teaming und einem Penetrationstest?

Durch die Antworten auf die Frage der Unterschiede zu anderen Methoden soll herausgefunden werden, inwieweit sich die Methoden abgrenzen lassen. Der Unterschied von einem Penetrationstest kann anhand einer Metapher beschrieben werden:

Bei einem Penetrationstest sind eine oder mehrerer Türen oder Fenster von einem Haus im Fokus. Es wird bspw. an einer Tür gerüttelt oder versucht, sie einzutreten. Dies ist wichtig, um Schwachstellen einer Tür aufzudecken und diese im Nachgang abzusichern. Beim Red Teaming ist nicht nur eine oder mehrere Türen oder Fenster im Fokus, sondern das ganze Haus. Wenn es nicht möglich ist, in die Tür zu kommen, dann wird ein Stein in das Fenster geschmissen, der Nachbar gefragt, oder ein Hintereingang verwendet und nach weiteren Wegen gesucht, ins Haus zu kommen.

Mit dem Haus ist die Infrastruktur einer Organisation gemeint. Sinnbildlich für die Türen, Wände und Fenster sind IT-System, Menschen oder Anwendungen.

Im Vergleich wurde mehrmals genannt, das Red Teaming bei der Suche eher in die Tiefe und ein Penetrationstests in die Breite geht. Red Teaming orientiert sich an den Prozessen und Zielen. Der Penetrationstest ist an bestimmte Objekte gebunden. Beim Red Teaming soll ein Weg zu einem spezifizierten Ziel erreicht werden. Im Penetrationstest dagegen sollen möglichst alle Schwachstellen gefunden werden. Das Red Team sucht nach den nützlichen Schwachstellen, die dabei helfen, näher ans Ziel zu kommen. Der Auftraggeber hat beim Red Teaming in der Regel das Hauptziel, die Erkennungs- und Reaktionsfähigkeit zu überprüfen. Der Penetrationstests prüft die Sicherheit von einem oder mehrerer Assets, wie einer Webanwendung oder IT-System. Das Red Team dagegen simuliert Angriffe von einer Angreifer-Gruppe. Der Penetrationstest simuliert einen Hackerangriff eines Einzeltäters und hat einen eingeschränkten Scope. Das Red Team ist in der Perspektive einer Angreifer-Gruppe, die gezielt eine oder mehrere Schwachstellen ausnutzen möchte, um an ein vorgegebenes Ziel zu kommen. Beim Penetrationstest dagegen sollen Schwachstellen nachgewiesen werden. Dabei muss eine Schwachstelle nicht unbedingt ausgenutzt werden. Häufig reicht ein Nachweis, dass eine Schwachstelle ausnutzbar ist. Der Scope wird beim Red Teaming häufig als offen bezeichnet. In den Gesprächen kam aber auch heraus, dass gewisse Einschränkungen gemacht werden. Beim Red Teaming wird in der Regel keine oder nur wenig Informationen an das Red Team übergeben. Das Red Team hat oft große Freiheiten und der Angriff erfolgt unangekündigt, manuell, verdeckt, unauffällig, leise und langsam. Der Penetrationstest bekommt dagegen gewisse Informationen, wie die IP-Adresse des Zielsystems übermittelt. Ein Penetrationstester ist auf die vorgegebenen Assets eingeschränkt, angekündigt und teilweise erfolgt eine Prüfung nach genauen Kundenanforderung. Die Prüfung ist eine Kombination aus automatisierten Tests, durch Schwachstellen- und Portscanner und manuellen Tests. Ein Test ist offensichtlich erkennbar. Im Red Teaming können sowohl technische und physische Sicherheit wie auch Social Engineering Angriffe durchgeführt werden. Ein Penetrationstest beschränkt sich im

Normalfall auf eine technische Prüfung. Das Red Teaming ist an der Managementebene angesiedelt und von dieser beauftragt. Als Ergebnis erhält das Management die erfolgreichen Angriffswege dokumentiert. Der Penetrationstest ist eher in einer fachlichen Führungsebene oder bei einem Sicherheitsbeauftragten angesiedelt, der die Verantwortung für bestimmte Assets hat und diese überprüfen möchte. Das Ergebnis ist eine Auflistung der Schwachstellen.

Mit folgender Tabelle werden die genannten Unterschiede tabellarisch dargestellt. Dabei ist zu beachten, dass dies eine nur sehr oberflächliche Betrachtung ist und es, wie in Kapitel 4.2.1.1 beschrieben, sehr große Unterschiede in Red Teaming Projekten gibt. Die Tabelle kann damit nicht bei jeder Kategorie eine für alle Projekte gültige Aussage treffen.

Tabelle 12: Penetrationstest vs. Red Teaming

	Red Teaming	Penetrationstest
Suche	Tiefensuche	Breitensuche
Eigenschaft	prozessorientiert/ zielorientiert	objektorientiert
Ziele Prüfer	festgelegtes Ziel erreichen/ Weg zum Ziel finden	möglichst alle Schwachstellen finden
Fokus	nur die nützlichen/ ausnutzbaren Schwachstellen aufdecken	möglichst alle Schwachstellen finden
Perspektive	Sicht einer Angreifer-Gruppe, die Schwachstellen ausnutzen möchte	Sicht eines Penetrationstesters, der alle Schwachstellen finden möchte
Angriffe	APT/ Angriffe von einer Angreifer-Gruppe simulieren	Angriff eines Einzeltäters simulieren
Scope	ganzheitlich/ offen/ eingeschränkt	eingeschränkt auf Objekte
Informationen	es werden keine Informationen übermittelt	bestimmte Informationen werden zur Verfügung gestellt
Ankündigung	unangekündigt	angekündigt
Freiheiten	Freiheiten/ eingeschränkt	eingeschränkt
Vorgehensweise	manuell/ verdeckt/ unauffällig/ leise und langsam	automatisiert und manuell/ offensichtlich
Techniken	technisch, physisch, Social Engineering	technisch
Ebene	Management	fachliche Führungsebene/ Sicherheitsbeauftragte
Ergebnis	Angriffswege	Schwachstellen

Der Unterschied der Methoden lässt sich anhand einer SQL-Injection Schwachstelle von einer Webanwendung verdeutlichen. Diese Schwachstelle ermöglicht es, einem Angreifer aufgrund unzureichender Überprüfung der eingegebenen Werte SQL-Befehle an eine

Webanwendung zu übergeben und so gültige Datenbankbefehle auszuführen. Daher hat ein Unberechtigter unter Umständen die Möglichkeit, unberechtigt Daten zu lesen, zu ändern oder zu löschen. Eine SQL-Injection Schwachstelle von einem Login kann bspw. dazu verwendet werden, eine Authentifizierung zu umgehen. Die SQL-Schwachstelle würde bei der Überprüfung der Webanwendung wahrscheinlich bei beiden Methoden gefunden werden. Beim Penetrationstest reicht es aus, nachzuweisen, dass eine Schwachstelle vorhanden bzw. diese ausnutzbar ist. Dagegen wird im Red Teaming versucht die Schwachstelle auszunutzen, um auf weitere Systeme zu kommen. Es ist auch zu beachten, dass beim Penetrationstest Schwachstellen als kritisch gesehen werden, diese im Red Teaming gar nicht beachtet werden oder nur eine geringe Bedeutung haben.

4.2.1.6 Gemeinsamkeiten – Was sind Gemeinsamkeiten von einem Red Teaming und einem Penetrationstest?

Als Gemeinsamkeiten wurden von den Interviewteilnehmern folgende Angaben gemacht:

- Bei beiden Methoden wird versucht, Schwachstellen aufzudecken.
- grundlegende Expertisen der Prüfer sind gleich
- Das Skillset/Level der Prüfer überschneidet sich oder ist gleich.
- Es wird ein Report geschrieben (aber der Inhalt ist unterschiedlich).
- Die Vorgehensweise, Techniken, Prozesse und Methoden sind sehr ähnlich.
- ein Scope wird definiert
- Viele Tools und Software können bei beiden Testweisen eingesetzt werden.
- Die initiale Kompromittierung ist oft gleich.

Bei kleinen und kritischen Infrastrukturen und rein technischen Tests wurde behauptet, dass Vieles zwischen einem Penetrationstest und Red Teaming gleich abläuft. Bei diesen Unternehmen fehlen häufig ein SOC, Netzwerksegmentierung und Security-Awareness-Maßnahmen. Dadurch können auch Tools aus dem Penetrationstest-Bereich, wie ein Port- oder Schwachstellenscanner, eingesetzt werden.

4.2.1.7 Vorteile – Welche Vorteile hat ein Red Teaming? Warum sollte ein Unternehmen ein Red Teaming durchführen?

Auf die Fragen, welche Vorteile ein Red Teaming hat und warum in einem Unternehmen ein Red Teaming durchgeführt werden sollte, zielt diese Kategorie ab. Bei der Frage nach den Vorteilen wurden folgende Aspekte genannt:

- Erkennungs- und Reaktionsfähigkeit des Blue Teams bei Angriffen wird verbessert
- Training für die Verteidigung bzw. das Blue Team
- realitätsnaher Angriff, indem viele unbewusste Schwachstellen aufgedeckt und behoben werden
- realitätsnahe Angriffsszenarien werden abgebildet und simuliert
- Prüfung, ob die Prozesse bei einem Sicherheitsvorfall funktionieren
- Schwachstellen werden behoben und Prozesse verbessert

- die Sicherheitsmechanismen/ -maßnahmen und deren Funktionsweise werden überprüft
- Die komplette Sicherheitskette wird überprüft, d. h. es besteht nicht nur eine technische Sichtweise, es werden auch Personen, Prozesse und die physische Sicherheit getestet.
- Es wird genutzt, um mehr Budget für die Security zu bekommen und herauszufinden, wo mehr investiert werden muss bzw. ob es sinnvoll eingesetzt wird.
- Die Auswirkungen von einem Sicherheitsvorfall werden veranschaulicht.
- Angriffswege werden dargestellt
- Es dient zum Vergleich mit anderen Unternehmen.
- Das Business und die Prozesse stehen im Fokus.
- Red Teaming kann zur Steigerung der Security Awareness führen.
- Es lässt sich prüfen, ob das Unternehmen in der Lage ist, einen Angreifer und den Angriff vollständig und nachhaltig zu entfernen.

Ein Interviewter hat bekräftigt, dass aufgrund der hohen Komplexität, Zero Day Exploits und Phishing in einem Unternehmen nie eine hundertprozentige Sicherheit gewährleistet werden kann. Es ist nicht möglich alle Endpunkte zu überwachen. Jedes Unternehmen muss damit rechnen, dass ein Angriff erfolgreich sein kann. Beim Red Teaming liegt daher der Fokus auf die Detektion und Reaktion von Angriffen.

4.2.1.8 Nachteile – Welche Nachteile hat die Durchführung eines Red Teaming?

Die Nachteile, die ein Dienstleister von Red Teaming sieht, sollen mit dieser Frage beantwortet werden. Die Aussagen im Fragenteil Nachteile wurde in drei Kategorien eingeteilt.

Voraussetzungen

Es wurde mehrmals genannt, das Red Teaming für Unternehmen, die bereits einen hohen Reifegrad der Informationssicherheit haben, zu empfehlen ist, d. h. bereits umfangreiche Maßnahmen und Sicherheitsüberprüfungen, wie Audits, Penetrationstests oder Vulnerability Management umgesetzt wurden. Bei Unternehmen, die keinen hohen Reifegrad haben und ein Red Teaming durchführen, würde der Mehrwert von vielen als gering angesehen und dem Unternehmen bspw. Empfohlen werden, einen Penetrationstest oder ein Audit durchzuführen.

Ebenfalls wurde mehrfach genannt, dass ein Red Teaming erst durchgeführt werden sollte, wenn ein Blue Team vorhanden ist, das zur Erkennung von Angriffen spezialisiert ist. Wenn kein Blue Team vorhanden ist sollten die Ressourcen anstatt in ein Red Teaming in Sicherheitsmaßnahmen, wie z. B. dem Aufbau eines Blue Teams investiert werden, so die Aussage einiger Gesprächspartner.

Bei einem Red Teaming ist es wichtig, auch ethische Aspekte zu beachten. Aus diesem Grund sehen es manche Dienstleister als sinnvoll an, die eigenen ethischen Regelungen festzuhalten.

Herausforderungen
Nach Aussagen von Interviewpartner ist es schwierig, herauszufinden, welcher Dienstleister wirklich gut und das Geld wert ist. Für Red Teaming ist eine hohe Expertise notwendig und es sollte eine Kommunikation zwischen Red und Blue Team stattfinden, wofür eine gewisse Erfahrung notwendig ist.

Bei vielen Kunden besteht eine Unklarheit zwischen Red Teaming und Penetrationstests. Damit der Kunde nicht ein anderes Ergebnis bekommt, als erwartet, ist die initiale Kommunikation sehr wichtig. In dieser muss diesem die Abgrenzung von Red Teaming aufgezeigt werden.

Aufgrund des breiten Scopes, gibt es in einem Test viele unterschiedliche Interessengruppen, auf die eingegangen werden muss. Daher ist die Kommunikation im Vergleich zum Penetrationstest häufig schwieriger und eine größere Herausforderung. Dabei muss vor allem das Blue Team von dem Test überzeugt werden. Es hat sich als hilfreich herausgestellt, Workshops im Nachgang mit dem Red und Blue Team durchzuführen.

Die Auswirkung aus einem Red Teaming kann sehr stark sein. Aufgrund von einem Ergebnis können große Investitionen in die IT-Sicherheit oder gar ein Umbau von Gebäuden erforderlich werden.

Nachteile
Als der Hauptnachteil von Red Teaming wird von den meisten gesehen, dass ein Red Teaming sehr aufwändig und daher kosten- und zeitintensiv ist.

Im Vergleich zum Penetrationstest wird mehr Zeit für Planung, Durchführung und Nachbereitung benötigt. In der Testdurchführung wird versucht, einen Weg zum Ziel zu finden. Dabei wird meistens nur ein Einstiegspunkt verwendet, nicht nach rechts und links geschaut und andere „blinde Flecken“ übersehen, da dies nicht im Fokus des Tests liegt. Es werden nur einzelne Schwachstellen ausgenutzt und nicht einzelne Systeme ausführlich getestet. Ein Red Teaming Assessment ist daher nicht zum initialen Assessment einer Organisation geeignet.

Durch ein Red Teaming kann keine vernünftige Aussage über die Verteidigungsfähigkeit von der Sicherheit im Unternehmen getroffen werden, da ein kleiner Fehler bereits ausreicht, um gewisse Sicherheitsmaßnahmen zu umgehen.

Bei Unternehmen, die einen hohen Reifegrad an IT-Sicherheit besitzen, kann es sein, dass ein Test nur wenige neue Erkenntnisse liefert, da bereits viele Schwachstellen bekannt sind.

Ein Red Teaming kann für schlechte Stimmung im Unternehmen sorgen, da nicht jeder die Testmethodik für sinnvoll hält. Dabei kann es auch zu internen politischen Streitereien im Unternehmen kommen, da unterschiedliche Bereiche in einem Unternehmen verschiedene Ziele verfolgen. Ein Red Teaming betrifft teilweise mehrere Bereiche eines Unternehmens, was ein Konfliktpotential birgt.

Generell gilt, dass ein Red Teaming nur etwas bringt, wenn man daraus lernt und sich weiterentwickelt. Dies ist nicht immer der Fall.

4.2.1.9 Risiken – Welche Risiken hat die Durchführung eines Red Teaming?

In dieser Kategorie sollen Risiken herausgefunden und die Erfahrungen der Mitarbeiter bei Red Teaming Projekte erfragt werden. Bei den Risiken wurde nach allgemeinen Risiken, aber auch zu Erfahrungen bei technischen, physischen und Social Engineering Angriffen gefragt.

Bei den technischen Prüfungen wurde nach kritischen Systemausfällen gefragt. Kein Dienstleister hat darüber berichtet, dass es zu einem kritischen Ausfall kam und ein hoher finanzieller Schaden entstanden ist. Es wurde lediglich von einzelnen Systemausfällen berichtet. Auch das Abmelden von Benutzern wird praktiziert, um zu prüfen, wie er darauf reagiert. Das Risiko zu einem kritischen Ausfall ist im Vergleich zu vielen Penetrationstests jedoch deutlich höher, da Angriffe in Produktivumgebungen durchgeführt werden.

Ein Sicherheitspersonal, das ein Gebäude vor Eindringlingen schützt, ist darin geschult, bei einem Angriff im Zweifel körperliche Gewalt oder Waffen anzuwenden. Dadurch, dass im Normalfall von einem Sicherheitspersonal nicht über ein Red Teaming Assessment informiert wird, kann ein Test nicht von einem realen Angriff unterschieden werden. Aus diesem Grund kann es bei einem Physical Assessment zur Gefahr für Leib und Leben oder einer Verhaftung des Red Teams kommen. Es wurden diesbezüglich aber noch keine negativen Erfahrungen gemacht.

Es wurde berichtet, dass ein Social Engineering Angriff zur Unzufriedenheit von Mitarbeitern geführt hat und im Nachgang Mitarbeiter gekündigt haben. Durch Social Engineering werden menschliche Eigenschaften von einzelnen Mitarbeitern gezielt ausgenutzt, dadurch kann es dazu kommen, dass einzelne Mitarbeiter schlecht dastehen und sich hintergangen fühlen. Das Vertrauen von Mitarbeitern zu einem Unternehmen kann beeinträchtigt werden. Es kann während des Tests zu ungeplanten Ereignissen kommen. So wurde bspw. eine Spear-Phishing E-Mail, die an einen Mitarbeiter verschickt wurde, an alle Mitarbeiter im Unternehmen weitergeleitet und hat so für größeres Aufsehen gesorgt.

Aufgrund dessen, dass heutzutage viele Cloudanbieter und gehostete Services genutzt werden, kann es aufwändig sein, die Genehmigung von allen Drittparteien einzuholen. Aufgrund von Unwissenheit und Unklarheiten kann dies zu rechtlichen Problemen und einer Haftung für ein Vergehen kommen.

Die Infrastruktur wieder in einen Ursprungszustand zurückzuführen, kann eine Herausforderung darstellen und es besteht das Risiko, dass dies nicht immer gewährleistet werden kann.

Von den Dienstleistern werden viele Maßnahmen ergriffen, damit die Risiken minimiert oder mitigiert werden, wie bspw.:

- Das Management wird in die Verantwortung von einem Red Teaming gezogen.

- Das Management wird dazu verpflichten, dass es keine Konsequenzen für einzelne Mitarbeiter gibt.
- Im Reporting wird großer Wert auf Datenschutz und den Schutz einzelner Mitarbeiter gelegt. Die Anonymität der Mitarbeiter wird gewahrt.
- Auf Angriffe bzw. Exploits, die die Verfügbarkeit gefährden, wird verzichtet
- Exploits oder das Ausführen von PoC auf kritischen Systemen erfolgt unter Abstimmung mit dem Kunden oder es wird auf ein Testsystem ausgewichen. Es wird darauf geachtet, dass Backups vorhanden sind.
- Die Mitarbeiter bekommen gewisse Informationen über einen Test übermitteln. Das Ergebnis wird dadurch nach Einschätzung nur gering verfälscht und die Akzeptanz der Mitarbeiter ist wesentlich höher.
- Es wird eine vorsichtige Vorgehensweise gewählt. Teilweise reicht es dem Auftraggeber aus, wenn ein Nachweis besteht, dass eine Schwachstelle ausnutzbar ist und die Schwachstelle nicht ausgenutzt wird.
- Die Risiken und wie damit umgegangen wird, wird im Vorfeld mit dem Kunden besprochen.
- Im Vorfeld werden Rahmenbedingungen mit dem Kunden abgestimmt.
- Es wird eine kontinuierliche Risikoanalyse durchgeführt und mit dem Kunden abgestimmt.
- Bei Fehlern und Störungen wird der Kunde bei der Behebung unterstützt.
- Es erfolgt eine Abstimmung mit dem Betriebsrat.

Zusammenfassend:

- Es kann zur Beeinträchtigung der Verfügbarkeit, Integrität und Vertraulichkeit kommen.
- Kritische Ausfälle von Live Produktivsystemen können zu einem (finanziellen) Schaden führen.
- Die Tester gehen bei eine Physical Assessment ein gewisses Risiko eines personellen Schadens ein.
- Social Engineering Angriffe können zur Unzufriedenheit von Mitarbeitern, Kündigungen und erheblichem Vertrauensverlust in das Unternehmen führen.
- Die Risiken sind zwar höher, da viele Tests in Produktivsystemen durchgeführt werden, aufgrund umfangreicher Maßnahmen und der vorsichtigen Vorgehensweise der Dienstleister sind die Risiken nach deren Aussage tragbar.

4.2.1.10 Sonstiges – Warum sollte ein Unternehmen Red Teaming bei Ihnen durchführen? Können Sie Referenzkunden nennen, die ein Red Teaming bei Ihnen durchgeführt haben? Welche Kunden führen ein Red Teaming durch?

Der letzte Block zielt darauf ab, Referenzkunden herauszubekommen, die bereits ein Red Teaming mit dem Dienstleister durchgeführt haben. Falls diese Frage nicht beantwortet werden kann, wird nach der Branche gefragt, in der die Kunden liegen, die Red Teaming durchführen. Die Antworten sollen auch Aufschluss geben, warum Red Teaming bei einem

bestimmten Anbieter durchgeführt werden sollte. Auf die Frage, warum ein Unternehmen bei den befragten Dienstleistern Red Teaming durchgeführt hat, folgten folgende Antworten:

- Es wird ein konstruktiver Ansatz gewählt und versucht, die Dinge vernünftig und richtig zu tun.
- Bei den Projekten wird auf die Bedürfnisse des Kunden eingegangen. Es ist eine Dienstleistung, die auf den Kunden hin geschnitten sind.
- Die offene Kommunikation steht im Mittelpunkt.
- Es ist ein sehr breiter Wissensschatz und Erfahrung im Unternehmen verfügbar.
- Eine hohe technische Expertise, z. B. beim Exploiting, wird zur Verfügung gestellt.
- Es gibt ein sehr breites Angebot an Sicherheitsdienstleistungen im Unternehmen.
- Ein umfangreiches und langjährig aufgebautes Wissen im Bereich Penetrationstests oder in der IT-Sicherheit ist vorhanden.
- Es sind umfangreiche Kennnisse über Bedrohungsmodelle vorhanden.
- Das Unternehmen besitzt viele Experten in unterschiedlichen Themenbereichen der IT-Sicherheit.
- Der Dienstleister konzentriert sich auf die Themengebiete Red Teaming und Penetrationstests.
- Es kann eine Verbindung zwischen Standards wie ISO/IEC 27001 und IT-Grundschutz und Red Teaming hergestellt werden.
- Das Unternehmen gehört zu den größten Sicherheitsdienstleistern.
- Es ist eine Forensik-Abteilung vorhanden, die das Blue Team unterstützen kann.
- Das Unternehmen hat sich schon seit langer Zeit mit Red Teaming beschäftigt und konnte bereits umfangreiche Erfahrungen sammeln.

Die Antworten der Dienstleister, welche Kunden Red Teaming durchführen, sind sehr unterschiedlich ausgefallen. Es gibt Dienstleister, die Red Teaming ...

- … nur bei nationalen Kunden ...
- … bei nationalen und internationalen Kunden ...
- … meistens in der Finanzbranche und im Bankensektor ...
- … hauptsächlich bei mittelständischen Unternehmen ...
- … in großen Unternehmen und Konzernen ...
- … in vielen unterschiedlichen Branchen (Gesundheitsbereich, Energiesektor, Pharma, Automobilindustrie, Recycling, öffentlichen Bereichen uvm.) ...
- … in kritischen Infrastrukturen ...

… durchgeführt haben.

Unter den befragten Dienstleistern hatten manche vor der Befragung nur wenige Projekte durchgeführt. Andere hatten bereits viele Projekte und langfristige Erfahrung in diesem Bereich gesammelt. Es wurde mehrmals genannt, dass aktuell keine Akquise notwendig ist, da die Kunden auf die Dienstleister mit Aufträgen zukommen. Red Teaming wird von vielen noch in der Entwicklungsphase gesehen, die aus dem Finanzsektor und dem Bankenumfeld

kommt. Diese Unternehmen suchen aktuell häufig nach Unterstützung bei der Vorbereitung und dem Aufbau von Red Teaming nach dem TIBER-EU Framework.

Die Dienstleister geben den Kunden das Versprechen, keine Kundennamen zu veröffentlichen. Aus diesem Grund hat kein Dienstleister einen Referenzkunden genannt. Dies ist unter Umständen auch darauf zurückzuführen, dass Dienstleister zum Teil erst wenige Projekte durchgeführt haben.

4.2.2 Fragenkatalog Auftraggeber

In der zweiten Befragung soll es darum gehen, Informationen auf Seiten des Auftraggebers zu erheben. Aus den bisherigen Gesprächen ging hervor, dass der Markt für Red Teaming noch sehr klein ist und aktuell im Wachsen ist. Zudem wird Red Teaming aufgrund des großen Aufwands und den Kosten nur von wenigen Unternehmen durchgeführt. Bei der Befragung der Dienstleister durfte kein Interviewteilnehmer einen Kunden nennen. Da auch Unternehmen, die Red Teaming durchgeführt haben, dies in der Regel nicht öffentlich bekannt geben oder auf der Webseite des Unternehmens ausschreiben, war es schwierig, Teilnehmer für die Befragung zu finden.

Zuerst wurde ein Aufruf bei XING gestartet. Ebenfalls wurden per E-Mail CERTS angefragt, die Red Teaming unter Umständen als Training für das Team durchführen. Zudem wurden Führungskräfte von Banken angeschrieben. Zusätzlich gab es persönliche Anfragen bei unterschiedlichen Personen auf Konferenzen. Aus der Interviewakquise haben sich drei Interviews ergeben. Bei zwei der drei Befragten wird Red Teaming innerhalb einer Organisation durchgeführt. Der Dritte hat einen Dienstleister beauftragt.

Die Ergebnisse aus den Interviews befinden sich im Anhang Anlage 3.

4.2.2.1 Gründe / Ziele

Die erste Frage zielt darauf ab, warum Red Teaming durchgeführt wurde. Die Ziele, die mit Red Teaming erreicht werden und was man damit erreichen wollte. Ein Befragter hat geantwortet, dass bereits Schwachstellenanalysen, Audits und Penetrationstests durchgeführt werden. Bei einem Penetrationstest wird ein White-Box-Ansatz gewählt, in dem der Tester auf Dokumentationen der zu testenden Systeme zugreifen kann. Red Teaming wird als Ergänzung zum White-Box-Test gesehen und im Black-Box-Verfahren durchgeführt. Mit Red Teaming sollen "blinde Flecken" aufgedeckt und das Red und Blue Team trainiert werden. Durch ein White-Team werden die Vorteile von einem White- und Black-Box-Test kombiniert.

Mit Red Teaming soll überprüft werden, ob bestimmte Angriffe und TTPs erkannt werden und wie weit ein Angreifer damit kommen würde.

Bei Führungskräften ist häufig die Denkweise verankert, dass der Kauf eines Security-Produktes einen ausreichenden Schutz bietet. Das Red Teaming bzw. das Simulieren eines realen Angriffs kann dabei helfen, die Denkweise der Vorgesetzten zu ändern.

Heutzutage gibt es ein allgemeines Ressourcenproblem und viele Schwachstellen in einem Unternehmen, die auch zum Teil bereits bekannt sind. Damit diese behoben werden ist der Beweis, dass eine Schwachstelle ausnutzbar ist, hilfreich.

Nach Aussagen der Auftraggeber sollten bspw. folgende Ziele erreicht werden.

- Zugang von außen in ein Netzwerk erhalten und versuchen, die Rechte zu eskalieren
- Neben dem Technischen auch die Prozesse und Kommunikation bei einem Sicherheitsvorfall überprüfen
- testen, ob ein bestimmter Angriff erkannt wird
- Kundendaten erhalten oder in einen Zahlungsverkehr eingreifen
- einen Weg finden, um ein festgelegtes Ziel zu erreichen

4.2.2.2 Positive Auswirkungen

Was hat das Red Teaming Projekt bewirkt, warum sollte man diese Methodik durchführen, und ob noch weitere Red Teaming Projekte durchgeführt werden, wird in der Kategorie positive Auswirkungen gefragt.

Mit Red Teaming wurden die gefunden Schwachstellen behoben und Prozesse optimiert. Es wurden Nachweise und Fakten über bestimmte Sicherheitsmängel geschaffen, die zu einem Umdenken bei verantwortlichen Personen gesorgt haben. Red Teaming ist hilfreich, da es realitätsnäher als ein Penetrationstest ist.

Es hat dabei geholfen, herauszufinden, wie gut und wie schnell auf einen Angriff reagiert wird und wie der Prozess verbessert werden kann.

Ein Interviewter hat davon berichtet, dass Server gefunden wurden, die noch nicht im Logging waren, oder ein anderer Server, auf dem ein unbekannter Benutzer angemeldet war.

Von allen befragten wird auch in Zukunft Red Teaming durchgeführt.

4.2.2.3 Negative Auswirkungen

Bei einem technischen Test kann es zu Systemabstürzen kommen. Auch Social Engineering birgt Gefahren. Daher wurde in dieser Kategorie nach negativen Auswirkungen bei den Auftraggebern gefragt.

Aufgrund eines sehr detaillierten ISMS und der durchzuführenden Prozesse, kann es dazu kommen, dass bei einem Sicherheitsvorfall nicht alle Schritte korrekt ausgeführt werden, was zu Problemen führen kann. Bei den Befragten wurde noch kein größerer Schaden angerichtet und es wurden keine negativen Erfahrungen mit Social Engineering gemacht. Es gab lediglich Auswirkungen auf die Verfügbarkeit, da ein Mitarbeiter mit einem realen Angriff gerechnet hat und daher einen Webserver abgeschaltet hatte.

Ein Gesprächspartner hat über einen Fall in den USA berichtet. In diesem wurde in den Medien über einen Angriff auf eine Organisation berichtet, obwohl es eigentlich ein vereinbartes Red Teaming gewesen war.[101]

4.2.2.4 Dienstleister

In der letzten Frage geht es darum, mit welchen Dienstleistern das Projekt durchgeführt wurde, wie dieser ausgewählt wurde und ob man mit dem Ergebnis zufrieden war.

Zwei der drei Befragten beauftragten interne Red Teams. Das Unternehmen, das einen Dienstleister ausgewählt hatte, war mit dem Ergebnis zufrieden. Der Mitarbeiter konnte nicht darüber berichten, wie der Dienstleister ausgewählt wurde.

4.2.3 Fazit

Die Dienstleister führen unter Red Teaming sehr unterschiedliche Sicherheitstests durch, welche sich je nach Kunde und Projekte unterscheiden können. Die Ausprägungen können in die Kategorien „*bedrohungsbasiertes*“ und „*informations-/ wissensbasiertes*“ Red Teaming aufgeteilt werden. Im Red Teaming werden Ziele festgelegt, die je nach Unternehmen individuell sein können, aber in der Regel die „Kronjuwelen“, d. h. unternehmenskritische Prozesse/ Funktionen, sensible Informationen oder Systeme betreffen. Der Ablauf und die Prozesse unterscheiden sich ebenfalls je nach Dienstleister. Sie können aber in die Phasen Vorbereitung, Durchführung und Abschluss aufgeteilt werden. Die Dauer und die Teamgröße sind ebenfalls sehr unterschiedlich. Bei den meisten haben sich eine Teamgröße von zwei Mitarbeitern im Red Team etabliert, je nach Aufgabenstellung werden zusätzliche Spezialisten in das Projekt integriert. Zwischen Red Teaming und Penetrationstests gibt es viele Gemeinsamkeiten, sowie Vor- und Nachteile. Je nach abgestimmter Vorgehensweise, können diese auch sehr unterschiedlich ausfallen. Die Tests werden in Live Produktivumgebungen durchgeführt, wodurch gewisse Risiken entstehen. Durch Kommunikation, Risikoanalyse und vielen weiteren Maßnahmen, wird versucht das Eintreten von vorhandenen Risiken zu minimieren. Ein großer Treiber für Red Teaming kommt aus dem Finanzsektor und Bankenumfeld. Die unterschiedlichen Dienstleister haben aber sehr unterschiedliche Kunden und Branchen genannt, sodass in vielen Sektoren bereits Red Teaming Projekte durchgeführt wurden.

Von den Auftraggebern wird Red Teaming als ergänzende Maßnahme zu Penetrationstests gesehen. Zudem werden die Ergebnisse genutzt, die Denkweise im Unternehmen zu verändern und zu entscheiden, für welche Maßnahmen das Budget eingesetzt wird. Den Auftraggebern geht es darum, herauszufinden, ob ein simulierter Angriff erkannt und wie darauf reagiert wird. Durch Red Teaming wurden Schwachstellen behoben, Prozesse optimiert und zusätzliche Sicherheitsmaßnahmen umgesetzt. Beim Red Teaming kann es zur Beeinträchtigung der Verfügbarkeit kommen. Es ist nicht zu größeren finanziellen Schäden,

[101] Vgl. *Sjouwerman, S.*, Democratic National Committee Thought it was Under Attack (It Was A Red Team Phishing Test…).

Abstürzen von kritischen Systemen oder weitreichende Auswirkungen von Social Engineering Angriffen bei den befragten Organisationen gekommen.

5 Methodik zur Einordnung der Prüfmethoden

In den Interviews wurde mehrfach genannt, dass Kunden sich beim Dienstleister gemeldet haben und ein Red Teaming durchführen wollten, obwohl ein Penetrationstest eine bessere Wahl für den Kunden gewesen wäre. Eine solche Problematik ist auch aus dem Penetrationstest bekannt. Dort wollen die Kunden bspw. den Stand der Informationssicherheit des Unternehmens wissen. Ein Penetrationstest gibt aufgrund dessen, dass normalerweise ein enger Scope gesetzt wird, nur begrenzt Auskunft darüber. In diesem Fall wird bspw. ein Cyber-Sicherheits-Check oder ISMS-Beratungsdienstleistungen nach ISO/IEC 27001 oder IT-Grundschutz empfohlen.

Der Geschäftsführer von einem IT-Sicherheitsdienstleister beschreibt in einem c't-Artikel, dass bei der aktiven Suche nach Einbruchsmöglichkeiten früher immer von einem Penetrationstest gesprochen wurde, bei dem Sicherheitsbarrieren durchbrochen und penetriert werden. Heute kommen die Begriffe Red Teaming beziehungsweise Red Team Assessment in Mode.[102] Mit diesen Aussagen wird eine Problematik zum Ausdruck gebracht, die im Rahmen dieser Arbeit ebenfalls aufgefallen ist. Aufgrund dessen, dass es keine einheitliche Vorgehensweise und Standardisierung der Begrifflichkeiten gibt, kann es dazu führen, dass ein Penetrationstest auch als Red Teaming verkauft wird oder umgekehrt. Auch die Beauftragung des Auftraggebers führt häufig zu einem eng gesetzten Scope, sodass bei manchen ein Red Team Assessment nahezu einem Penetrationstest entspricht.

In diesem Kapitel werden die Methoden Audit, Penetrationstest und Red Teaming direkt miteinander verglichen. Es wird versucht, eine Methodik zur Einordnung zu erarbeiten.

5.1 Vergleich der Methodiken

> Bei einem Penetrationstest (…) ist meist ein klarer Fokus auf bestimmte Zielobjekte vorgegeben und ein klarer Rahmen festgesteckt, in dem sich die Prüfer bewegen. Sie versuchen mit den Techniken und Werkzeugen eines Hackers möglichst alle Schwachstellen im vorgegebenen Rahmen zu finden. Der Auftraggeber soll so eine möglichst vollständige Bewertung der Sicherheit des zu betrachtenden Ziels bekommen, um danach die Schwachstellen beheben zu können. Bei einem Red Team Assessment wird dagegen ein realistischer Angriff eines Hackers simuliert, dem es nicht auf die Vollständigkeit ankommt. Ihm reicht eine Schwachstelle aus, um die Kontrolle über einen Arbeitsplatz seines Ziels zu bekommen und von dort aus auf interessante Daten oder Server zuzugreifen beziehungsweise weiter angreifen zu können. Dabei stehen ihm alle Mittel und Wegen offen. Dazu gehört insbesondere auch der physische Zugang oder sogar Einbruch in die Räumlichkeiten des Ziels, die Platzierung von spezieller Hardware im Netzwerk des Opfers, um zum Beispiel eine Hintertür über UMTS zu hinterlassen oder die Täuschung von Mitarbeitern.[103]

So wurde der Unterschied in einer Fachzeitschrift erläutert. Um einen Vergleich zwischen den Methodiken zu ziehen, werden Annahmen auf Grundlage der Klassifizierung vom BSI

[102] Vgl. *Strobel, S.*, Sprechen Sie Security?, S. 79.
[103] *Strobel, S.*, Sprechen Sie Security?, S. 79.

(siehe Kapitel 2.9.3 Klassifikation) getroffen. In der Tabelle 13: Klassifizierung Red Teaming, Penetrationstest und Audit nach dem BSI werden die Unterschied, die im Folgenden Text erläutert werden, aufgezählt.

Red Teaming und Penetrationstests können als White- oder Black-Box-Test ausgeführt werden. Bei einem Audit werden Prozesse und Dokumente von einer Infrastruktur betrachtet und ausführliche Informationen mit dem Auftraggeber ausgetauscht. Daher wird es in dieser Arbeit als White-Box-Ansatz bezeichnet.

Beim Red Teaming und Penetrationstest kann von einer Aggressivität des Testers zwischen abwägend und vorsichtig ausgegangen werden. Das Audit ist passiv scannend. Mit passiv scannend ist in diesem Zusammenhang kein technischer Scan gemeint, sondern das Überprüfen von Dokumenten und Konfigurationen.

Beim Umfang von einem Red Teaming und Audit Projekt wurde das Adjektiv vollständig gewählt. Damit soll ausgedrückt werden, dass nicht alle Systeme überprüft werden, sondern, dass alle Systeme im Scope liegen und Schwachstellen davon ausgenutzt werden können. Beim Audit wird eine qualitative Stichprobe gewählt, die ein möglichst vollständiges Bild vermittelt. Im Penetrationstest ist der Umfang dagegen häufig begrenzt oder fokussiert auf einzelne Systeme, Dienste oder ein Netz.

Im Gegensatz zum Audit und Penetrationstest wird beim Red Teaming versucht, verdeckt zu bleiben, damit ein Angriff nicht direkt erkannt wird. Das Red Teaming kann sowohl durch einen Netzwerkzugang, sonstige Kommunikation, physischer Zugang oder Social Engineering durchgeführt werden. Der Penetrationstest erfolgt in den meisten Fällen über einen Netzwerkzugang oder eine sonstige Kommunikation, wie dem WLAN. Im Audit werden Audittechniken wie die Dokumentenprüfung eingesetzt, um Nachweise zu sammeln.

Sowohl Red Teaming als auch ein Penetrationstest kann sowohl von außen als auch von innen durchgeführt werden. Beim Audit wurde „von innen“ gewählt, da ein Auditor sich Informationen im Unternehmen anschaut und bspw. eine geführte Besichtigung macht. Der Vergleich wird mit der Tabelle 13: Klassifizierung Red Teaming, Penetrationstest und Audit nach dem BSI verdeutlicht.

Tabelle 13: Klassifizierung Red Teaming, Penetrationstest und Audit nach dem BSI

Kriterium	Red Teaming	Penetrationstest	Audit
Informationsbasis	Black-Box/ White-Box	Black-Box/ White-Box	White-Box
Aggressivität	abwägend/ vorsichtig	abwägend/ vorsichtig	passiv scannend
Umfang	vollständig	begrenzt/ fokussiert	vollständig
Vorgehensweise	verdeckt	offensichtlich	offensichtlich

Kriterium	Red Teaming	Penetrationstest	Audit
Technik	Netzwerkzugang/ sonstige Kommunikation/ physischer Zugang/ Social Engineering	Netzwerkzugang/ sonstige Kommunikation	Audittechniken
Ausgangspunkt	von außen/ von innen	von außen/ von innen	von innen

Im nächsten Schritt werden die Methodiken auf Grundlage mehrere Kriterien verglichen. Als Basis wird die aus der Primärforschung generierten Unterschiede zwischen Penetrationstests und Red Teaming verwendet (siehe Kapitel 4.2.1.5) und Audits auf Grundlage der theoretischen Grundlage Kapitel 2.8 Audit ergänzt.

Das Audit ist im Vergleich zum Penetrationstest und Red Teaming ebenfalls in die Breite ausgelegt und orientiert sich an den gegebenen Informationen. Es werden die Anforderungen aus dem Standard überprüft. Im Fokus liegt, die Konformitäten bzw. die Abweichungen zu einem Standard herauszufinden. Dazu wird eine qualitative Stichprobe verwendet, die möglichst vollständig die Anforderungen des Standards überprüft. Bei einem initialen Audit ist der Vollständigkeitsanspruch meistens nicht zu erfüllen, da nur Stichproben verwendet werden können. Dies ergibt sich erst durch regelmäßige Audits. Der Scope kann sowohl auf der ganzen Organisation als auch auf einen bestimmten Bereich eingeschränkt sein. Der Auditor schaut sich die dazugehörigen Prozesse an und lässt sich die notwendigen Informationen von einer Organisation, in Form von Dokumenten oder Interviews, übermitteln. Der Auditor hat Freiheiten bei der Wahl der Stichprobe und den Audittechniken und führt Prüfungen manuell durch. Ein Audit wird angekündigt und ist dem Unternehmen bekannt. Das Ziel, warum ein Audit durchgeführt wird, ist in der Regel die Konformität zu einem Standard, mit dem der Stand der Informationssicherheit festgestellt werden kann. Ein Audit sollte auf Managementebene angesiedelt sein. Häufig liegt die Verantwortung eher auf einer fachlichen Führungsebene (z. B. Chief Security Officer) oder bei einem Sicherheitsbeauftragten. Das Ergebnis ist ein Bericht über die Konformitäten bzw. den Abweichungen gegenüber dem Standard. Es werden keine Angriffe in einem Audit durchgeführt.

Tabelle 14: Vergleich zwischen Red Teaming, Penetrationstests und Audit

	Red Teaming	Penetrationstests	Audit
Suche	Tiefensuche	Breitensuche	Breitensuche
Eigenschaft	prozessorientiert/ zielorientiert	objektorientiert	informations-orientiert/ standardorientiert / anforderungs-orientiert

	Red Teaming	Penetrationstests	Audit
Ziele Prüfer	festgelegtes Ziel erreichen/ Weg zum Ziel finden	möglichst alle Schwachstellen finden	Konformität zu einem Standard prüfen
Fokus	nur die nützlichen/ ausnutzbaren Schwachstellen aufdecken	möglichst alle Schwachstellen finden	Konformität/ Abweichungen zu einem Standard feststellen
Perspektive	Sicht einer Angreifer-Gruppe, die Schwachstellen ausnutzen möchte	Sicht eines Penetrationstesters, der alle Schwachstellen finden möchte	Sicht eines Auditors, der Konformitäten aufdecken möchte
Angriffe	APT/ Angriffe von einer Angreifer-Gruppe simulieren	Angriff von einem Einzeltäter simulieren	-
Scope	ganzheitlich/ offen/ eingeschränkt	eingeschränkt auf Objekte	ganzheitlich/ eingeschränkt
Informationen	Es werden keine Informationen übermittelt.	Bestimmte Informationen werden zur Verfügung gestellt.	Alle für das Audit angeforderten Informationen werden zur Verfügung gestellt.
Ankündigung	unangekündigt	angekündigt	angekündigt
Freiheiten	Freiheiten/ eingeschränkt	eingeschränkt	Freiheiten
Vorgehensweise	manuell/ verdeckt/ unauffällig/ leise und langsam	automatisiert und manuell/ offensichtlich	manuell
Techniken	technisch, physisch, Social Engineering	technisch	Audittechniken
Ebene	Management	fachliche Führungsebene/ Sicherheits-beauftragte	Management/ fachliche Führungsebene/ Sicherheits-beauftragte
Ergebnis	Angriffswege/ Schwachstellen	Schwachstellen	Konformitäten/ Abweichungen

5.2 Methodik zur Einordnung

Im vorherigen Kapitel wurde ein Vergleich zwischen Red Teaming, Penetrationstests und Audits gezogen. Dieses Kapitel wird eine Methodik entwickelt, die verwendet werden kann, um als Unternehmen einzuordnen, in welchem Fall welche Methodik als sinnvoll erscheint.

Im ersten Schritt muss sich ein Unternehmen damit beschäftigen, welche Ziele es mit einer Sicherheitsüberprüfung erreichen möchte. In der Tabelle 15: Ziele der Methodiken sind die Hauptziele der Methoden benannt, die dabei helfen können, sich für eine Methodik zu entscheiden.

Tabelle 15: Ziele der Methodiken

	Red Teaming	Penetrationstest	Audit
Mögliche Ziele	- Erkennung und Reaktion auf Sicherheitsvorfälle prüfen - Verbesserung der Widerstands-fähigkeit von Unternehmen gegen Cyber-Angriffe - Das Blue Team trainieren - „Blinde Flecken“ aufdecken	- möglichst alle Schwachstellen aufdecken - Risikograd einer oder mehrerer Assets feststellen	- Stand der Informations-sicherheit prüfen - Konformität/ Abweichungen zu einem Standard feststellen

Anschließend muss sich ein Unternehmen bewusst machen, was und in welchem Umfang getestet werden soll. Ein Red Teaming und Audit verfolgt tendenziell einen ganzheitlichen Ansatz. Beim Penetrationstest hingegen sollen gezielt ein oder mehrere Assets (z. B. IT-Systeme oder Anwendungen) auf Schwachstellen überprüft werden. Beispiele, wie auf Grundlage vom Scope und der Ziele die Methodik ausgewählt wird, soll mit den Beispielen in der Tabelle 16: Methodik Beispiele verdeutlicht werden.

Tabelle 16: Methodik Beispiele

Methodik	Beispiel
Red Teaming	Ein Unternehmen möchte einen ganzheitlichen Sicherheitstest durchführen, bei dem die Erkennung und Reaktion auf einen Sicherheitsvorfall geprüft wird.
Penetrationstest	Ein Unternehmen möchte bei einer Webanwendung herausfinden, ob Schwachstellen vorhanden sind und wie hoch deren Risikograd ist.
Audit	Ein Unternehmen möchte herausfinden, wie der Stand der Informationssicherheit im Unternehmen ist.

Neben den Zielen und dem Scope ist der Reifegrad eines Unternehmens ein empfehlenswerter Indikator zur Wahl der Methodik. Bekräftigt wird dies durch einen

Vortrag mit dem Titel „*Red teaming probably ins't for you*". In diesem wird erläutert, dass die meisten Unternehmen kein Red Teaming benötigten, bevor sie nicht ein Vulnerability Management (dt. Schwachstellenmanagement), eine Log-Sammlung, -Analyse, -Response und einen funktionierenden Penetrationstest und Behebungsprozess etabliert haben.[104] Bei einem Vulnerability Management wird eine Infrastruktur regelmäßig automatisiert auf bekannte Schwachstellen überprüft, um Schwachstellen aufzudecken und anschließend zu beheben. Das automatische Prüfen einer Infrastruktur auf Schwachstellen wird auch als Schwachstellenscan bezeichnet.

Auch beim Penetrationstest sollten gewisse Schritte vorher erfolgt sein. So wird im Blog-Artikel *„Penetrationstest vs. Schwachstellenscan: Wann Sie die richtige Wahl treffen"* beschrieben, dass ein Penetrationstest, der eine Sicherheitslücke aufdeckt, die sonst unbemerkt geblieben wäre, auf den ersten Blick sein Geld wert ist. Bei genauer Betrachtung hätte die Sicherheitslücke aber mit erheblich weniger Aufwand gefunden, beseitigt und das Geld effizienter eingesetzt werden können. Kostspielige Penetrationstests wahllos über eine gesamte IT-Infrastruktur durchzuführen, würde bedeuten, andere wichtige Schritte, wie ein Patch- und Schwachstellenmanagement, falls noch nicht vorhanden, zu überspringen. Als ein wirtschaftlicher und sicherer Weg wird empfohlen, im ersten Schritt ein Patchmanagement für alle Systeme umzusetzen. Der zweite Schritt ist ein umfassendes Schwachstellen-Management mit regelmäßigen Scans, die systematische Lücken im Patchmanagement aufspüren. Erst im dritten Schritt sollten Penetrationstests gemacht werden, bei denen gezielt bestimmte Systeme überprüft werden.[105]

Der Artikel mit dem Titel *„When to Use Vulnerability Assessments, Pentesting, Red Teams, and Bug Bounties"* wird ebenfalls eine bestimmte Schrittfolge festgelegt.[106] Bei einem Bug Bounty-Programm wird für das Finden von Schwachstellen bei einem Produkt (z. B. einer Webanwendung) eine Belohnung ausbezahlt. Dadurch, dass quasi jeder versuchen kann, Schwachstellen von einem Produkt zu finden, kann ein Produkt von vielen Analysten betrachtet und untersucht werden. Der Autor des Artikels sieht folgende Schritte als sinnvoll an:

1. Haben Sie einen vertrauenswürdigen Berater (eine Person oder ein Unternehmen), der Ihre Bemühungen zur Sicherheitsbewertung über Ihre Reifegrade hinweg steuern kann.
2. Beginnen Sie mit Vulnerability Assessment und führen Sie keine der anderen Arten von Tests durch, bis Sie Ihre Umgebung durch Behebung soweit bereinigt haben, sodass es schwierig ist, Dinge zu finden.
3. Dann wechseln Sie zu Penetrationstests mit einem vertrauenswürdigen Unternehmen.
4. Wenn Sie keine Ergebnisse mehr von vertrauenswürdigen Penetrationstests erhalten, sollten Sie ein Bug-Bounty-Programm hinzufügen, um "vielen Augen" zu nutzen.
5. Nachdem die Phase mit Vulnerability Assessment abgeschlossen ist, sollten Sie sich, wenn Sie in die Penetrationstest-Phase eintreten, auch mit Red Teaming auseinandersetzen, und zwar nicht nur, weil es einige Zeit dauern wird, zu recherchieren und gute Optionen zu finden. Red Teams sind keine

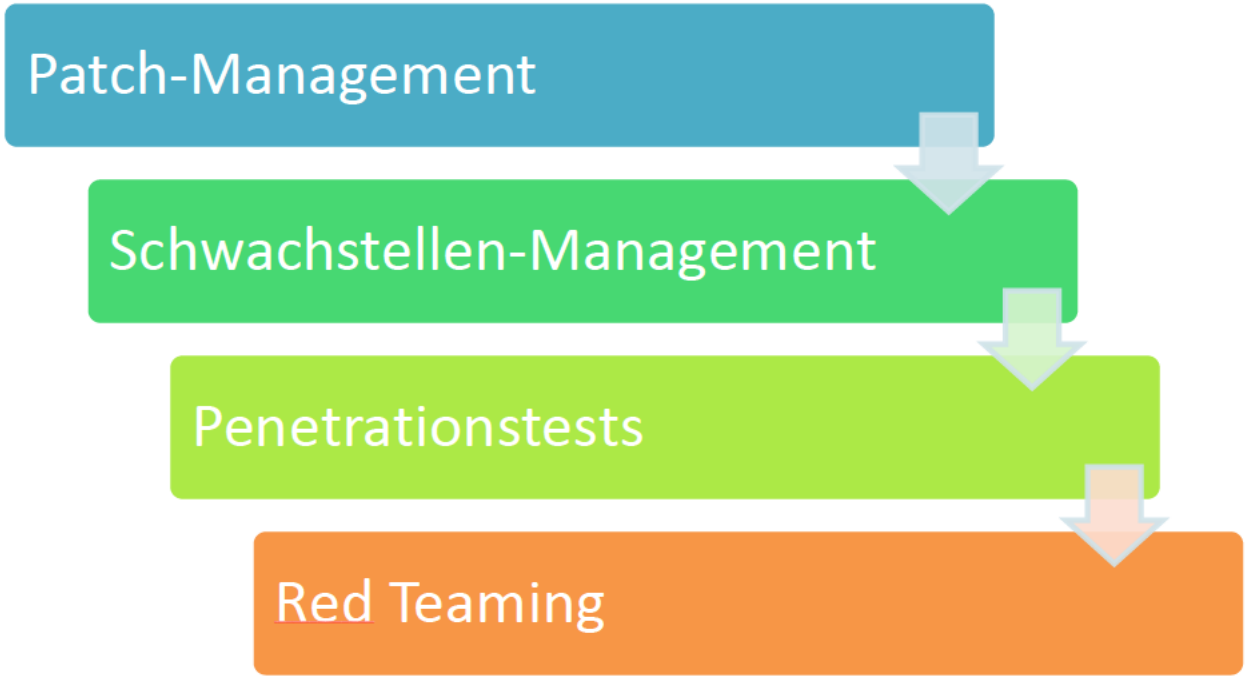
[104] Vgl. *Kohlenberg, T.*, Red teaming probably isn't for you, 2017.
[105] Vgl. *Brabetz, S.*, Penetrationstest vs. Schwachstellenscan: Wann Sie die richtige Wahl treffen, 2016.
[106] Vgl. *Miessler, D.*, When to Use Vulnerability Assessments, Pentesting, Red Teams, and Bug Bounties, 2016.

"besseren" Penetrationstests; sie sind eine ganz andere Art der Bewertung, mit unterschiedlichen Zielen.

6. Denken Sie daran, dass Sie von Ihrem/n vertrauenswürdigen Berater(n) durch all dies geführt werden; es gibt viele Variablen, die bestimmen, wann und wie Sie was tun. [107]

Aus diesem Artikel heraus wurde folgende Treppe entwickelt (siehe Abbildung 23: Sicherheitstreppe).

Abbildung 23: Sicherheitstreppe I



Um ein Audit durchzuführen, muss ein bestimmter Standard ausgewählt werden, auf dessen Grundlage die Konformität geprüft wird. Zudem kann mit einem Audit der Reifegrad der Informationssicherheit festgestellt werden. Die Audits geben Aufschluss darüber, welche Sicherheitsmaßnahmen notwendig sind, um die Anforderungen an einen Standard zu erfüllen oder ein Risiko für ein Unternehmen tragbar zu machen.

Alternativ zu einem Audit könnte ein Sicherheitsberater durch seine Expertise dabei unterstützen, den Reifegrad bspw. durch einen Workshop oder Beratungsgespräch zu bestimmen, um grundlegende Sicherheitsmaßnahmen zu erkennen und umzusetzen. Eine individuelle Beratungsleistung, die nicht auf einen Standard beruht, ist stark abhängig von der Erfahrung und dem Wissen des Beraters. Aufgrund dessen, dass ein Audit ein standardisiertes Vorgehen hat und die Auditoren dafür ausgebildet wurden, ist ein solches Verfahren vorzuziehen. Aus den genannten Gründen könnte eine Abfolge von Schritten auch wie folgt aussehen (siehe Abbildung 24: Sicherheitstreppe II):

[107] *Miessler, D.*, When to Use Vulnerability Assessments, Pentesting, Red Teams, and Bug Bounties, 2016.

Abbildung 24: Sicherheitstreppe II

Eine Abstufung von Reifegraden würde nach den recherchierten Informationen ergeben, dass für Red Teaming ein hoher Reifegrad, für Penetrationstest ein mittlerer und für Audits ein niedriger oder keiner erforderlich ist. Es ist zwar z. B. beim CSC (siehe Kapitel 2.8.2) kein bestimmter Reifegrad erforderlich, doch ist zu beachten, dass, wenn bspw. ein ISO/IEC 27001-Zertifizierung angestrebt wird, bestimmte Anforderungen erfüllt werden müssen, damit ein Zertifikat erreicht wird. Die Erkenntnisse wurden in der Tabelle 17: Reifegrad zusammengefasst.

Tabelle 17: Reifegrad

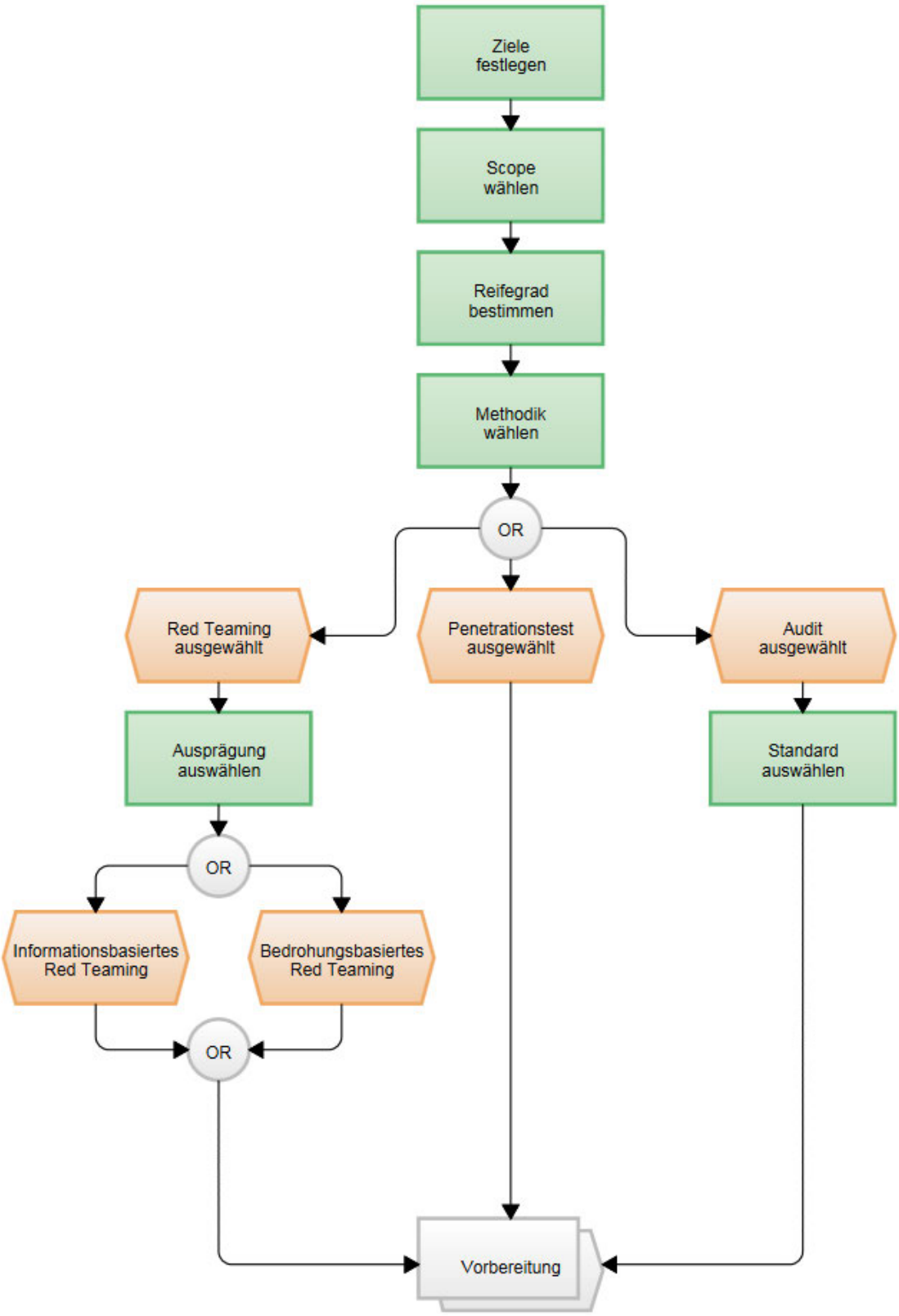
Methodik	Reifegrad	Einstufung
Red Teaming	Es ist empfohlen, z. B. ein Patch- und Schwachstellen-Management, eine Log-Analyse, -Sammlung, -Response sowie einen funktionierenden Penetrationstest und Behebungsprozess etabliert zu haben.	hoch
Penetrationstest	Es ist empfohlen, z. B. zuerst ein Patch- und Schwachstellen-Management einzuführen, sodass mit geringem Aufwand viele Schwachstellen geschlossen und aufgedeckt werden können.	mittel
Audit	Beim CSC ist kein bestimmter Reifegrad erforderlich. Zum Erreichen eines Zertifikats müssen die Anforderungen von einem Standard erfüllt werden.	niedrig

Die unterschiedlichen Methodiken schließen sich nicht gegenseitig aus, doch ist das Budget oft begrenzt, sodass nicht alle gleichzeitig oder nacheinander durchgeführt werden können.

In dieser Arbeit liegt der Fokus auf Red Teaming, Penetrationstest und Audits. Neben den genannten Methodiken gibt es noch weitere, wie bspw. eine Source-Code-Analyse, die je nach Situation hilfreich sein können.

Der Prozess wurde als EPK visualisiert (siehe Abbildung 25: EPK Methodik zur Einordnung) und endet mit der Vorbereitungsphase (siehe Kapitel 6.6.1). Triviale Ereignisse, bspw. dass eine Funktion abgeschlossen ist, wurden weggelassen.

Abbildung 25: EPK Methodik zur Einordnung



5.3 Unternehmensprofile

Durch die erarbeiteten Grundlagen wurden Unternehmensprofile/ Stereotypen erarbeitet, die dabei helfen sollen, ein Unternehmen einzuordnen.

Das erste Unternehmensprofil *„bedrohungsbasiertes Red Teaming“* beschreibt ein Unternehmen, das Red Teaming durchführen könnte (siehe Tabelle 18: Unternehmensprofil bedrohungsbasiertes Red Teaming). Für diese Methodik ist ein gewisser Reifegrad erforderlich, wie in Kapitel 5.2 bereits erläutert. Eine weitere Voraussetzung ist eine Bedrohungsanalyse, die bestimmte Bedrohungen für ein Unternehmen beschreibt. Diese wird im Rahmen des Assessments durchgeführt – oder wurde bereits durchgeführt – und dient als Grundlage. Um eine initiale Bewertung einer Organisation zu erhalten, ist die Methodik nicht geeignet, da gezielt nur einzelne Schwachstellen ausgenutzt oder Angriffsszenarien betrachtet werden. Die Dauer ist je nach Dienstleister und Projekt sehr unterschiedlich. Im Vergleich zum Penetrationstest und Audit ist die Dauer als lang und die Kosten als hoch anzusehen. Aufgrund der hohen Kosten ist ein solcher Test vor allem interessant, wenn es um eine Infrastruktur (Informationen, Daten, Maschinen) geht, die einen sehr hohen Schutzbedarf besitzt und ein Angriff für einen hohen (finanziellen) Schaden führen würde, wie es bspw. bei einer kritischen Infrastruktur oder im Finanzsektor wäre. Die Verteidigung einer solchen Infrastruktur durch ein unangekündigtes Red Teaming auf bestimmte Bedrohungen zu prüfen, wäre nachvollziehbar. Bei der Unternehmensgröße kann davon ausgegangen werden, dass ein bedrohungsbasiertes Red Teaming eher für mittelständischen oder großen Unternehmen mit den notwendigen finanziellen Mitteln hilfreich und umsetzbar ist. Für Unternehmen, die zum Finanzsektor gehören und voraussichtlich in Zukunft das TIBER-EU Framework umsetzen müssen, ist ebenfalls zu empfehlen, sich mit der Umsetzung zu beschäftigen.

Tabelle 18: Unternehmensprofil bedrohungsbasiertes Red Teaming

Unternehmensprofil bedrohungsbasiertes Red Teaming	
Mögliche Voraussetzung	Das Unternehmen hat einen gewissen Reifegrad in der Informationssicherheit erreicht. Dies wurde durch eine Zertifizierung mit einem Standard, z. B. der ISO 27001 oder IT-Grundschutz, erreicht. Maßnahmen, wie z. B. ein Patch- und Konfigurationsmanagement, Vulnerability Management, Penetrationstests, Audits, Security Awareness und weitere wurden bereits etabliert. Das Unternehmen hat eine besonders schützenswerte Infrastruktur, bei der ein Angriff einen besonders hohen (finanziellen) Schaden anrichten würde. Um sich vor bestimmten Bedrohungen zu schützen, soll eine Bedrohungsanalyse durchgeführt werden bzw. wurde bereits durchgeführt. Daraus wurden/ werden Threat Models, Angriffsszenarien und Angriffe identifiziert. Nach dieser Analyse

Unternehmensprofil bedrohungsbasiertes Red Teaming	
	werden/ wurden Maßnahmen eingerichtet, um sich vor bestimmten Bedrohungen zu schützen.
Initiales Assessment	nicht geeignet
Dauer	lang
Kosten	hoch
Unternehmensgröße	mittel bis groß

Beim zweiten Profil wird ein Red Teaming ohne Bedrohungsanalyse durchgeführt, bei dem keine bestimmte APTs oder Angreifer-Gruppen abgebildet werden (siehe Tabelle 19: Unternehmensprofi). Dadurch kann die Dauer eines Projektes kleiner und mit geringerem Aufwand verbunden sein, wie diese bei einem bedrohungsbasierten Red Teaming wäre, da die Bedrohungsanalyse entfällt. Wie im ersten Profil beschrieben, ist auch hier ein gewisser Reifegrad sinnvoll (siehe Kapitel 5.2). Im Vergleich zum Penetrationstest ist die Dauer und sind die Kosten in der Regel höher, da das Red Teaming im Unterschied häufig tiefer geht, die benötigten Mittel bereitgestellt und eine umfangreiche Informationssammlungsphase, wie ein OSINT durchgeführt wird. Dies wird heutzutage in den meisten Penetrationstests nicht gemacht. Diese alternative Methodik wird von Dienstleistern auch bei kleinen Unternehmen durchgeführt und kann hilfreich sein, „blinde Flecken", d. h. unbekannte Schwachstellen aufzudecken oder festzustellen, in welchem Bereich weitere Maßnahmen oder Investitionen notwendig sind. Es dient ebenfalls dazu, die Verteidigung vor Sicherheitsvorfällen zu prüfen. Bei kleineren Unternehmen gibt es häufig keine spezialisierten Teams für die Erkennung von Angriffen, die bspw. Log-Daten auswerten. Aus diesem Grund werden viele Angriffe nicht erkannt. Ein Bericht von einem solchen Test beschreibt einen erfolgreichen Angriffsweg, der dazu genutzt werden kann, Schwachstellen zu beheben. Da das Red Teaming versucht, sehr realitätsnah zu sein, kann es zu einem Umdenken bei Führungskräften führen, die häufig noch die Denkweise haben, dass ein Sicherheitsprodukt ausreicht, sich vor Angriffen zu schützen.

Tabelle 19: Unternehmensprofil informations-/wissensbasiertes Red Teaming

Unternehmensprofil Red Teaming	
Mögliche Voraussetzung	abweichend zum Unternehmensprofil „bedrohungsbasiertes Red Teaming" wird keine Bedrohungsanalyse durchgeführt
Initiales Assessment	nicht geeignet
Dauer	mittel bis lang
Kosten	mittel bis hoch
Unternehmensgröße	beliebig

Ein Penetrationstest kann dabei helfen ein oder mehrere Assets gezielt zu prüfen, um weitere Schwachstellen aufzudecken und das Sicherheitsniveau der Assets zu erhöhen (siehe Tabelle 20: Unternehmensprofil Penetrationstest). Der Penetrationstest kann für ein initiales Assessment nur bedingt genutzt werden, da in der Regel nur technische Aspekte betrachtet werden und die Kosten, um alle Systeme ausführlich zu prüfen, zu hoch sind. Um technisch die Systeme auf bekannte Schwachstellen zu überprüfen, eignet sich ein

Vulnerability Management. Bei diesem wird automatisiert geprüft und so können bereits mit geringerem Aufwand und niedrigeren Kosten viele bekannte Schwachstellen gefunden werden. Im Vergleich zum Red Teaming ist die Dauer und sind die Kosten in den meisten Fällen geringer als beim Red Teaming, da der Scope häufig eingeschränkter ist und gezielt überprüft wird. Zudem können zum Teil auch automatisierte Tools verwendet werden. Beim Red Teaming können automatisierte Tools nur selten verwendet werden, da diese schnell durch ein Blue Team erkannt werden könnten. Dadurch werden diese in der Regel nicht eingesetzt, was zu einem höheren Aufwand bzw. Kosten im Vergleich zum Penetrationstest führt. Auch eine Information Gathering Phase wird aufgrund der dafür benötigten Kosten häufig nicht beauftragt, was dadurch zu einer Ersparnis gegenüber einem Red Teaming führt. Ein Penetrationstest ist grundsätzlich für jede Unternehmensgröße durchführbar.

Tabelle 20: Unternehmensprofil Penetrationstest

Unternehmensprofil Penetrationstest	
Mögliche Voraussetzung	Es wird empfohlen bspw. ein Patch- und Schwachstellen-Management und weitere grundlegende Sicherheitsmaßnahmen bereits etabliert zu haben, damit Schwachstellen gefunden werden, die nicht schon mit geringerem Aufwand hätten gefunden werden können.
Initiales Assessment	bedingt geeignet
Dauer	kurz bis mittel
Kosten	gering bis mittel
Unternehmensgröße	beliebig

Das Audit, z. B. der CSC, ist besonders für ein initiales Assessment geeignet. Auch kleine Unternehmen, die noch kein ISMS und die dafür notwendigen Dokumentationen haben, können den CSC durchführen (siehe Kapitel 2.8.2). Ein Audit ist im Vergleich in den meisten Fällen kürzer und mit geringeren Kosten verbunden als ein Red Teaming. Dies ist aber stark abhängig vom verwendeten Standard und der Unternehmensgröße.

Tabelle 21: Unternehmensprofil Audit

Unternehmensprofil Audit	
Mögliche Voraussetzung	Beim CSC sind kein bestimmter Reifegrad bzw. keine Dokumente erforderlich. Zum Erreichen eines Zertifikats müssen die Anforderungen von einem Standard erfüllt werden.
Initiales Assessment	geeignet
Dauer	kurz bis mittel
Kosten	gering bis hoch
Unternehmensgröße	beliebig

5.4 Klassifizierung

In der Primärforschung konnte festgestellt werden, dass es eine Vielzahl von unterschiedlichen Ausprägungen gibt (siehe Kapitel 4.2.1.1). Dies ist auch beim

Penetrationstest der Fall. Aus diesem Grund hat das BSI für Penetrationstests einen Klassifizierungsbaum erstellt (siehe Kapitel 2.9.3), der bei der Spezifizierung eines Penetrationstests helfen kann.

Wenn ein Red Teaming auf Basis der Klassifizierung eines Penetrationstests durchgeführt wird, fehlen einige Kriterien, die ein Red Teaming charakterisieren können. Aus diesem Grund wurde folgende Tabelle entwickelt:

Tabelle 22: Klassifizierung Red Teaming

Kriterium		Kurze Beschreibung
Ausprägung Welche Art von Ausprägung wird verwendet?	bedrohungsbasierter	Test basiert auf Bedrohungsinformationen.
	informations-/ wissensbasierter	Test basiert auf einer Information-Gathering-Phase und der Expertise der Tester.
Angriffsweg Wie werden die Angriffe festgelegt?	frei	Die Tester haben freie Wahl der Angriffe.
	festgelegt	Die Angriffswege werden vor dem Test festgelegt.
	szenariobasiert	Es werden Szenarien beim Test festgelegt.
Ankündigung Sind die Tests angekündigt?	unangekündigt	Die Tests sind unangekündigt.
	angekündigt	Die Verteidigung wird über den Test informiert.
Unterstützung Wird die Verteidigung beim Test unterstützt	unterstützend	Die Verteidigung wird während dem Test unterstützt.
	ohne Unterstützung	Die Verteidigung wird während dem Test nicht unterstützt

Die Tabelle kann dazu verwendet werden, die Klassifizierung nach dem BSI (siehe Kapitel 2.9.3) zu ergänzen. Sie soll dabei helfen, auszuwählen und festzulegen, welche Art von Red Teaming durchgeführt wird und diese beschreiben.

5.5 Fazit

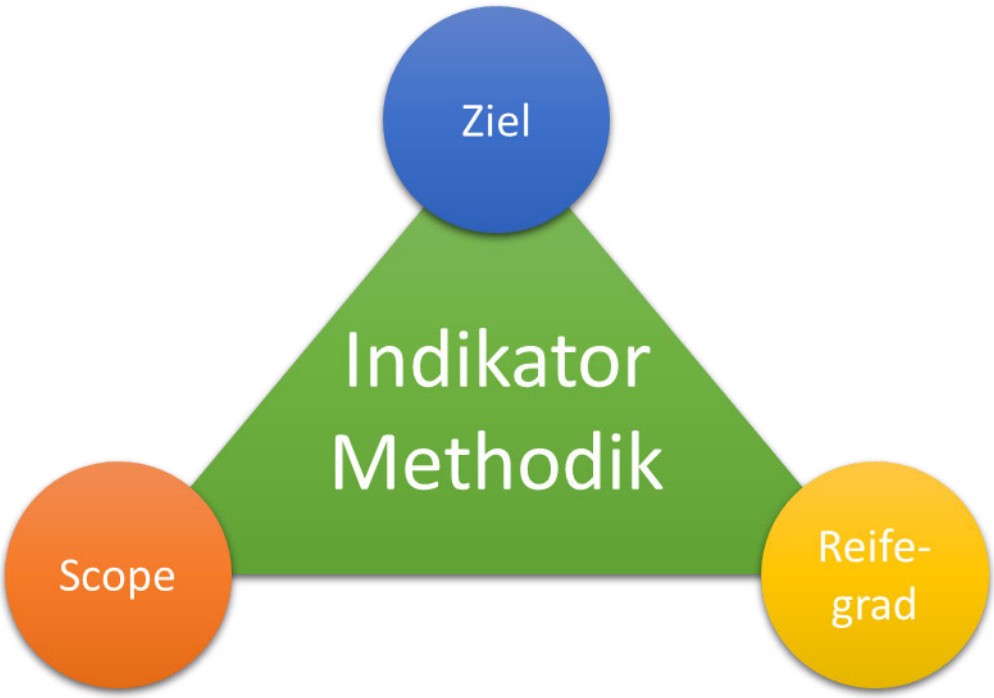
Abschließend zu diesem Kapitel wird auf den Blog Artikel „*Penetration Test vs. Red Team Assessment: The Age Old Debate of Pirates vs. Ninjas Continues*“ eingegangen. Dieser beschreibt sehr anschaulich die Unterschiede zwischen Penetrationstest und Red Teaming. Die auch im Rahmen vom Vergleich der Methodiken herausgearbeitet wurden. In diesem Artikel wird der Penetrationstester als die Piraten und Red Teamer als die Ninjas beschrieben, in der die Thematik zum Unterschied zwischen Red Teaming und Penetrationstests anschaulich beschrieben werden. Als Fazit wird gezogen, dass Penetrationstester und Red Teams häufig die gleichen Personen sind, die in eine unterschiedliche Rolle schlüpfen und unterschiedliche Methoden und Techniken für eine Bewertung einer Infrastruktur verwenden. Die wahre Antwort zwischen Penetrationstest

vs. Red Team ist dieselbe wie bei Piraten vs. Ninjas – einer ist nicht unbedingt besser als der andere und beide in einer bestimmten Situation nützlich. So würde man keine Piraten benutzen wollen, um heimliche Operationen durchzuführen und keine Ninjas, um die Meere auf der Suche nach Schätzen zu befahren. Mit einem Penetrationstest möchte man nicht beurteilen, wie gut die Reaktion auf einen Sicherheitsvorfall ist und Red Teaming wird nicht verwendet, um möglichst alle Schwachstellen aufzudecken.[108]

In dem Artikel werden keine Audits angesprochen, doch könnten diese ergänzt werden. Audits sind ebenfalls nicht besser oder schlechter, sondern für bestimmte Situationen und Voraussetzungen nützlich.

Als drei wichtige Indikatoren, um die Methodik auszuwählen, haben sich die Ziele, der Scope und der Reifegrad von einem Unternehmen herausgestellt. Dies wird mit der Abbildung 26: Indikator Methodik veranschaulicht.

Abbildung 26: Indikator Methodik



Auch eine gewisse Abfolge der unterschiedlichen Methodiken erscheint als empfehlenswert. Bspw. könnte zuerst ein Audit, mit dem der Reifegrad bestimmt wird, durchgeführt werden. Die vorgefundenen Abweichungen zum Standard aus dem Audit werden im Nachgang behoben. Auch kann man z. B. ein Patch- und Schwachstellenmanagement einsetzen, um viele Schwachstellen mit geringem Aufwand zu finden und zu beheben – bevor ein Penetrationstest durchgeführt wird. Das kann als nachvollziehbarer Schritt angesehen werden. Erst mit einem gewissen Reifegrad sollten Penetrationstests von bestimmten

[108] *Hayes, K.*, Penetration Test vs. Red Team Assessment: The Age Old Debate of Pirates vs. Ninjas Continues, 2016.

Assets, z. B. besonders kritischen IT-Systemen, oder Systeme mit sensiblen Daten, durchgeführt werden. Ein Angriff bspw. auf kritische Infrastrukturen könnte bei Erfolg zu einem hohen (finanziellen) Schaden führen. Erst wenn ein hoher Reifegrad bspw. durch Audits und Penetrationstest erreicht wurde, wird ein Red Teaming, dass unangekündigt das Blue Team testet, als praktikable Vorgehensweise angesehen.

Eine Klassifizierung für Penetrationstest reicht für ein Red Teaming nicht aus. Daher wurden die Kriterien Ausprägung, Angriffsweg, Ankündigungen und Unterstützung festgelegt, die eine Klassifizierung nach dem BSI ergänzen können. Eine solche Klassifizierung hilft dabei, ein Red Teaming genau zu spezifizieren.

6 Praktikable Methode zur Durchführung

Nach der Marktforschung wurden die Methodiken verglichen und ein Verfahren entwickelt, mit dem ein Bedarf eingeordnet werden kann. Eine auf das erarbeitete Wissen basierende Definition zu Red Teaming könnte wie folgt lauten:

„Red Teaming ist ein Sicherheitstest bei dem reale Angriffe simuliert werden. Das Red Team ist eine Gruppe, die versucht, durch Angriffe, die sowohl technische, physische und menschliche Komponenten betreffen können, an ein spezifiziertes Ziel, z. B. die „Kronjuwelen" des Unternehmens, d. h. kritische Geschäftsprozesse oder schützenswerte Informationen, zu kommen. Die Verteidigung, die auch als Blue Team bezeichnet wird, versucht die Angriffe zu erkennen und darauf zu reagieren. Das Blue Team ist nicht über den Test informiert. Die Schnittstelle zwischen dem Red und Blue Team ist das White Team, das über den Test informiert ist und Ansprechpartner für beide Teams ist. Das Hauptziel von Red Teaming ist die Erkennungs- und Reaktionsfähigkeit der Organisation auf einen Sicherheitsvorfall zu verbessern."

Auf Grundlage des bisher erarbeiteten Wissens soll eine praktikable Methode zur Durchführung von Red Teaming beschrieben werden. Aufgrund dessen, dass es viele Ausprägungen gibt und sich Red Teaming pro Projekt unterscheiden kann, ist es nicht möglich den einen methodisch korrekten Weg zu finden. Zudem sollte Red Teaming vor einer Durchführung immer kritisch hinterfragt werden, was mit folgenden Thesen gemacht wird. Aus den recherchierten Informationen wurden Thesen erarbeitet (siehe Kapitel 6.1), die anschließend begründet werden.

6.1 Thesen

Bereits 2013 wurde ein Whitepaper von SANS veröffentlich, das die Notwendigkeit von Red Teaming sieht und begründet (siehe Kapitel 2.10.1). Doch ist Red Teaming auch heute eine notwendige Methodik?

Auf Grundlage des gesammelten Wissens aus der Masterarbeit des Verfassers werden nachfolgend Thesen aufgestellt und begründet.

1. These: Auf Grund der aktuellen Bedrohungslage ist Red Teaming eine sinnvolle Ergänzung zu Penetrationstests und Audits.

Zu den am häufigsten vorkommenden Cyber-Bedrohungen gehören Malware, webbasierte- und Phishing-Angriffe. Daher sollten Unternehmen Schutzmaßnahmen für diese Bedrohungen einrichten und diese überprüfen. Beim Red Teaming wird häufig Malware eingesetzt oder nachgeahmt. Auch webbasierte Angriffe oder Phishing sind gängige Praxis im Assessment und spiegeln die Realität wieder. Es gibt verschiedene Bedrohungsklassen, die unterschiedlichen Fähigkeiten, Böswilligkeiten, Motivationen und Methoden haben

(siehe Kapitel 2.3). Wie sehr welches Unternehmen von welcher Bedrohung betroffen ist, kann bspw. durch eine Bedrohungsanalyse herausgefunden werden, um diese anschließend gezielt per Red Teaming zu testen.

Täglich werden mehr als 350.000 neue Schadprogramme registriert, d. h. ein Unternehmen hat die Herausforderung, sich davor zu schützen. Das BSI berichtet zusätzlich davon, dass es eine steigende Bedrohung von professionellen Angriffen, sogenannten APTs, gibt. Die durchschnittliche Verweildauer von einem Angreifer im Netzwerk beträgt 101 Tage (siehe Kapitel 2.5). Die lange Verweildauer von Angreifern und hohe Komplexität der Angriffe lässt darauf schließen, dass es nicht mehr ausreicht, sich auf Sicherheitsprüfungen, wie ein Penetrationstest oder ein Audit, zu verlassen. Zudem kann ein Unternehmen, wie es auch im Whitepaper von Microsoft beschrieben wird (siehe Kapitel 2.10.3), davon ausgehen, dass ein Angriff früher oder später erfolgreich ist. Aus diesem Grund kann die Notwendigkeit von Red Teaming gesehen werden, da dadurch aktuelle reale Bedrohungen simuliert und die Erkennungs- und Reaktionszeit der Verteidigung verbessert wird. Es kann auf diese Weise einem Unternehmen dabei helfen, auf einen Angriff besser vorbereitet zu sein.

Voraussetzung dafür ist, dass gewisse Sicherheitsmaßnahmen bereits umgesetzt sind (siehe Kapitel 5.2). Bei einer Infrastruktur bei der bestimmte Schutzmaßnahmen nicht vorhanden sind, hat ein Tester bzw. der Angreifer leichtes Spiel. Zudem ist der Mehrwert gering oder hätten mit geringerem Aufwand erreicht werden können. Wenn bspw. kein Patch-Management vorhanden ist, ist die Wahrscheinlichkeit hoch, dass in der Infrastruktur nicht alle Sicherheitsupdates installiert sind und so bekannte Schwachstellen vorhanden sind. Um herauszufinden, ob das Patch-Management Schwächen aufweist, ist ein Schwachstellen-Management bzw. ein Schwachstellen-Scan, der automatisiert IT-Systeme überprüft, empfehlenswert. Um dies herauszufinden ist kein Red Teaming notwendig, das unter Umständen mehrere Monate dauert.

Viele interne Angriffe können nur identifiziert werden, wenn ein Logging durchgeführt und Mechanismen zur Erkennung implementiert sind. Bevor ein Red Teaming durchgeführt wird, sollte hinterfragt werden, ob Sicherheitsmaßnahmen vorhanden sind, die das getestete Szenario erkennen können.

2. These: Red Teaming ist ein Nischenprodukt, das aktuell nur für wenige Unternehmen in Deutschland relevant ist bzw. einen Mehrwert bietet.

In Deutschland sind 99 Prozent der Unternehmen dem Mittelstand zuzuordnen. Dieser ist somit ein wesentlicher Faktor für die Wirtschaft. Es gibt mehrere Studien, die die IT-Sicherheit in kleinen und mittleren Unternehmen (KMU) bewerten. Bei KMU besteht häufig noch Nachholbedarf in vielen Bereichen der IT-Sicherheit.[109]

Bei einer Repräsentativbefragung „*Aktuelle Lage der IT-Sicherheit in KMU*“ vom Bundesamt für Wirtschaft und Energie (BMWI) wurde veröffentlicht, dass sich die Anstrengungen für

[109] Vgl. *BSI*, IT-Sicherheit in kleinen und mittleren Unternehmen (KMU), 2019.

IT-Sicherheit von 2011 bis 2017 nur wenig erhöht haben. Es sind zwar flächendeckend Basislösungen vorhanden, bei personellen und organisatorischen Maßnahmen bleiben die Unternehmen aber hinter der eigenen Risikoeinschätzung zurück. Kleine KMUs halten sogar einen Sicherheitsbeauftragten für nicht erforderlich und setzen stattdessen einen Mitarbeiter ein, der die Aufgaben wie IT, IT-Sicherheit und Datenschutz in Teilzeit mit anderen Aufgaben erfüllen muss.[110] Das in KMUs bereits ein Blue Team zur Angriffserkennung etabliert ist, ist voraussichtlich eher eine Ausnahme.

Auch meine persönliche Einschätzung auf Grundlage der gesammelten Erfahrung als IT-Sicherheitsberater lässt darauf schließen, dass die meisten KMUs noch einen niedrigen Reifegrad haben und zuerst ein funktionierendes ISMS und Sicherheitsprozesse, wie bspw. ein Patch-, Vulnerability-Management oder einen Schwachstellenbehebungsprozess aufbauen müssen.

Auch regelmäßige Audits und Penetrationstests werden eher in wenigen Unternehmen regelmäßig durchgeführt. Dies bekräftig auch die Bitkom-Studie bei der nur 24% der befragten Unternehmen Penetrationstests einsetzen.[111] Erst wenn diese Methodiken und Prozesse etabliert sind, sollte sich ein Unternehmen mit Red Teaming beschäftigen (siehe Kapitel 5.2).

Dadurch, dass KMUs in Deutschland 99% ausmachen, kann davon ausgegangen werden, dass Red Teaming nur für eine geringe Anzahl an Unternehmen relevant ist bzw. das Geld effizienter eingesetzt werden kann. Auf Grund der steigenden Bedrohungslage kann davon ausgegangen werden, dass Unternehmen weiter aufrüsten und der Reifegrad weiter ansteigt, sodass die Anzahl der KMUs, für die Red Teaming relevant ist, in Zukunft steigt.

Ein eigenes Red Team aufzubauen das Red Teaming durchführt oder einen Dienstleister zu beauftragen erzeugt einen großen Aufwand und hohe Kosten. Dies ist ein weiterer Grund warum Red Teaming nur von wenigen finanzstarken Unternehmen durchgeführt werden kann.

3. These: Es gibt nur wenige Dienstleister, die ein bedrohungsbasiertes Red Teaming, wie es in CREST oder TIBER-EU beschrieben wird, umsetzen. Die Ausprägung von Red Teaming wird von vielen im Rahmen von einem Projekt definiert.

Allgemein gab es mehrere Gesprächspartner, die erst einige wenige Projekte durchgeführt haben. Das bisherige Kerngeschäft liegt meistens in den Themenbereichen Penetrationstest, ISMS-Beratung oder weiteren IT-Sicherheitsdienstleistungen. Es gab nur wenige Dienstleister, die ein bedrohungsbasiertes Red Teaming durchführen. Nur wenige Unternehmen richten sich nach einem Standard, wie dem TIBER-EU und CREST, was auch darauf zurückzuführen ist, dass das TIBER Framework bspw. erst im Mai 2018 veröffentlicht wurde und die Nachfrage erst in den letzten Jahren aufgekommen ist. Der Großteil der

[110] Vgl. *Hillebrand, A.* u. a., Aktuelle Lage der IT-Sicherheit in KMU., S. 8, 14.
[111] Vgl. *Bitkom e.V.*, Spionage, Sabotage und Datendiebstahl - Wirtschaftsschutz in der Industrie., S. 38.

befragten Dienstleister führt Red Teaming als ein individuell auf einen Kunden zugeschnittenen Sicherheitstest, bei dem die Rahmenbedingungen im Projekt festgelegt werden, durch.

4. These: Der Aufwand, eine Bedrohungsanalyse durchzuführen, ist für die meisten Unternehmen in Deutschland nicht umsetzbar.

Auf der BSIDES in Stuttgart 2018 wurde in einem Vortrag über "*Cyber Threat Intelligence for Enterprise IT and Products*" berichtet. In der Präsentation wurde beschrieben, was Thread Intelligence (TI) ist und wie dies in einem Unternehmen aufgebaut werden kann.[112] Beim TI werden aktuelle Informationen zur Bedrohungslage der IT-Sicherheit durch Cyberangriffe und andere Gefahren geliefert. Hierzu werden Daten aus unterschiedlicher Quelle verwendet und in aufbereiteter Form zur Verfügung gestellt.[113] Der Vortragende berichtete, dass Unternehmen ganze Abteilungen mit diesem Thema beschäftigen oder in Zukunft aufbauen wollen. Im Rahmen dieser Arbeit kann nicht beantwortet werden, inwieweit es für ein Unternehmen erforderlich ist, sich selbst detailliert mit den eigenen Bedrohungen zu beschäftigen und ob ein solcher Aufwand zu rechtfertigen ist. Nach meiner Einschätzung sind der Aufwand und die Kosten nur für die wenigsten Unternehmen tragbar.

5. These: Beim Red Teaming reale Angriffe durchzuführen, ist eher unrealistisch. Es sind immer inszenierte Szenarios die zum Teil nur bedingt die Realität wiederspiegeln.

Bei einem Red Teaming sollen reale Angriffe simuliert werden. Dienstleister unterstellen sich eigenen ethischen Richtlinien und müssen rechtliche Rahmenbedingungen (siehe Kapitel 5 und Kapitel 3) einhalten. Im folgenden Abschnitt soll anhand eines inszenierten Szenarios verdeutlicht werden, warum ein Red Teaming unrealistisch ist.

Ein Red Team führt bei einem Red Teaming Projekt ein Physical Assessment durch. Bei der Besichtigung findet das Red Team im Gebäude eine Tür, hinter der sich vermutlich ein Serverraum befindet. Die Tür ist mit einem sicheren Schloss abgeriegelt und lässt sich nicht durch einfache Mittel öffnen, allerdings ist sie von so geringer Stärke, dass sie mit einer Brechstange aufgebrochen werden könnte. Ein realer Angreifer könnte sich überlegen sich als Feuerwehrmann mit einem Brecheisen zu verkleiden und den Feueralarm auszulösen. Die Ausnahmesituation könnte ausgenutzt werden, um die Tür unbemerkt aufzubrechen. Ein solches Vorgehen könnte bei einem gezielten realen Angriff und böswilliger Absicht ein durchaus denkbares Szenario sein. Beim Red Teaming würde aufgrund des finanziellen Schadens, der durch einen falsch ausgelösten Feueralarm und der Sachbeschädigung entsteht, ein solcher Angriff nicht durchgeführt.

Dies ist nur ein Beispiel, das verdeutlichen soll, dass es schwierig ist reale Angriffe abzubilden, da sich reale Angreifer nicht an ethische Regeln oder Gesetze halten. Bei einem technischen Angriff würde der reale Angreifer sich ebenfalls keine Gedanken machen, ob ein

[112] Vgl. *BSides Stuttgart*, BSides Stuttgart - Because Cyber has no Knautschzone.
[113] Vgl. *Luber, S./Schmitz, P.*, Was ist ein Threat Intelligence Service?, 2017.

Exploit die Verfügbarkeit der IT-Systeme beeinträchtigt oder nicht, sondern würde dies beabsichtigt oder unbeabsichtigt in Kauf nehmen und im Zweifel einen Schaden anrichten. Allgemein ist es somit nur bedingt möglich wirkliche Angreifer zu simulieren.

6. These: Red Teaming ohne ein Blue Team bzw. eine Verteidigung durchzuführen, ist nicht sinnvoll. Ein Audit sowie ein Penetrationstest sind in der Regel einem Red Teaming vorzuziehen.

In den Interviews wurde mehrmals mitgeteilt, dass ein Red Teaming nur bei einem bestimmten Reifegrad und einer bereits vorhandenen Verteidigung als sinnvoll angesehen und der Mehrwert bei einem Unternehmen mit niedrigem Reifegrad gering ist (siehe Kapitel 5.2). Aufgrund des Aufwands und der Kosten sollten andere Maßnahmen, wie ein Audit oder ein Penetrationstest, vorgezogen werden.

7. These: Red Teaming birgt ein großes Risiko für ein Unternehmen.

Durch ein Red Teaming kann es zur Beeinträchtigung der Schutzziele der Informationssicherheit kommen. Dadurch, dass ein Red Teaming in Live-Produktivumgebungen durchgeführt wird, kann ein Ausfall direkt zu einem Schaden führen. Wenn ein ERP-System nicht mehr erreichbar ist, von dem Produktionsprozesse abhängig sind, könnte es zu einen Produktionsstillstand kommen. Bei einer längeren Beeinträchtigung der Verfügbarkeit, können hohe Kosten für ein Unternehmen entstehen.

Auch das Red Team geht bei der Durchführung von einem Physical Assessment ein gewisses Risiko ein, das ein verantwortlicher Sicherheitsdienst falsch reagiert. Social Engineering Angriffe, die direkt den Menschen betreffen, können zur Unzufriedenheit, zur Kündigung und zu einem Vertrauensverlust an ein Unternehmen führen. Die Dienstleister sind sich den Risiken bewusst und versuchen diese durch unterschiedliche Maßnahmen tragbar zu machen, doch ist ein größerer (finanzieller) Schaden durch einen Test durchaus realistisch.

Trotzdem wurde bei den Gesprächen mit den Dienstleistern von keinem größeren Schaden berichtet. Es wurde sogar die Aussage getroffen, dass die Risiken aufgrund der Vorgehensweise vernachlässigbar sind. Die Gefahren die durch Sicherheitstest in einer Produktivumgebung auftreten, sollten sowohl vom Anbieter als auch vom Auftraggeber nicht unterschätzt werden.

In den Interviews wurde erwähnt, dass zum einen eine vorsichtige Vorgehensweise gewählt, und versucht auf Exploits zu verzichten, die die Verfügbarkeit gefährden können. Diese Aussage kann angezweifelt werden, da von vielen Dienstleistern bekannte Frameworks und Exploits verwendet werden. Sowohl die Exploits aus den Frameworks als auch selbstentwickelte Software durchlaufen nur selten Softwaretests, um eine hohe Qualität zu gewährleisten. Auch wenn die Software vor einem Einsatz getestet wurde, kann es aufgrund der hohen Komplexität in einer Infrastruktur immer zu einem unerwarteten verhalten kommen. Häufig sind die Exploits sogar nur ein Proof-of-Concept, dass die Ausnutzbarkeit beweisen soll. Ein Exploit hat in der Regel keinen Anspruch auf Funktionssicherheit und Stabilität. Daher ist allein der Einsatz von öffentlich verfügbaren Exploits und

selbstentwickelten Skripten ein Risiko, das unter Umständen zu einem (hohen) Schaden führen kann. Zudem kann es immer durch unbekannte oder unbedachte Risiken zu einem Schaden führen.

8. These: Aufgrund der Risiken sollte ein Red Teaming als White-Box-Test oder in einem mehrstufigen Vorgehen durchgeführt werden.

Folgende Aussage wurde im „*Praxis-Leitfaden für IS-Penetrationstest*“ vom BSI veröffentlicht und ist auf das Red Teaming in gewissem Maße übertragbar:

> Das BSI empfiehlt, grundsätzlich Whitebox-Tests durchzuführen, da bei einem Blackbox-Test aufgrund nicht vorliegender Informationen Schwachstellen übersehen werden können. Es besteht die Gefahr, dass im Rahmen eines Blackbox-Tests Szenarien wie der Angriff eines informierten Innentäters nicht berücksichtigt werden. Zusätzlich besteht bei einem Blackbox-Test ein höheres, durchaus vermeidbares Risiko, einen unbeabsichtigten Schaden zu verursachen. Darüber hinaus ist der Aufwand bei einem Blackbox-Test wesentlich größer als bei einem Whitebox-Test. Den Prüfern sollten daher nach Möglichkeit alle für die Testdurchführung notwendigen Informationen über die zu testenden Systeme zur Verfügung gestellt werden.[114]

Das Red Teaming birgt ein großes Risiko bei technischen, physischen und Social Engineering Angriffen, wie auch in der vorherigen These erläutert wurde. Trotzdem wird bei einem Red Teaming häufig ein Black-Box-Ansatz gewählt. Dadurch können Schwachstellen übersehen werden und auch das Risiko, einen Schaden zu verursachen, ist höher. Wenn ein Informationsaustausch zwischen dem Red und Blue Team stattfinden würde, wäre ein Angriff zwar nicht sehr realitätsnah, könnte aber bei vielen Szenarien ein möglicher Schaden vermieden werden. Ebenfalls ist ein Purple-Teaming, bei dem ein Red- und Blue-Team zusammenarbeiten, um die Erkennungs- und Reaktionszeit zu verbessern, ein gangbarer Weg, bevor ein unangekündigter Black-Box-Test durchgeführt wird.

In der „*Durchführungsstudie für Penetrationstest*“ vom BSI wird auch ein mehrstufiges Vorgehen empfohlen. Dieses beschreibt, dass zuerst ein vorsichtiger, verdeckter Black-Box-Test von außen und anschließend ein aggressiver, offensichtlicher White-Box-Test von innen durchgeführt wird. Mit diesem Vorgehen würden die Vorteile eines Black-Box- und White-Box-Test kombiniert. Der Vorteil vom Black-Box-Ansatz ist, dass ein möglichst realistischer echter Angriff simuliert wird und der White-Box Ansatz Vorteile hinsichtlich Effizienz und Schadensminimierung aufweist.[115] Ebenfalls ist ein Gray-Box-Test bei dem gewisse Informationen ausgetauscht werden empfehlenswerter als per Black-Box-Test mögliche Risiken in Kauf zu nehmen.

9. These: Wargaming ist das „bessere“ Red Teaming oder sollte mit diesem kombiniert werden.

Das Red Teaming mit einem War Gaming-Workshop zu kombinieren oder diesen separat durchzuführen, wie es im Microsoft Whitepaper beschrieben wird (siehe Kapitel 2.10.3), ist ein interessanter Ansatz. Bei einem solchen Termin werden bestimmte Sicherheitsvorfälle

[114] *BSI*, Ein Praxis-Leitfaden für IS-Penetrationstests, 2016., S. 5-6.
[115] *BSI*, Studie Durchführungskonzept für Penetrationstests., S. 17.

durchgespielt und Sicherheitsmaßnahmen kritisch hinterfragt. Wie beim Red Teaming gibt es ein Red Team, das sich Angriffe überlegt und ein Blue Team, das sich mit Verteidigungsmaßnahmen auskennt. Zum Unterschied vom Red Teaming werden diese nur in einer Diskussionsrunde besprochen und nicht real durchgeführt. Einen solchen Workshop mit Sicherheitsexperten durchzuführen, kann eine effiziente Methode darstellen und könnte Grundlage sein, im Nachgang vereinzelt Red Teaming für bestimmte Szenarien durchzuführen.

10. These: Um die physische oder personelle Sicherheit zu verbessern, sind andere Methoden sinnvoller.

In den Interviews wurde genannt, dass ein Ziel von Red Teaming war, die Security Awareness zu steigern. Diese Aussage trifft zu, allerdings gibt es bessere Methoden, die Security Awareness zu steigern, in dem unternehmensübergreifende Security Awareness Kampagnen durchgeführt werden, um im Unternehmen das Sicherheitsbewusstsein zu steigern. Darunter könnten bspw. Phishing-Kampagnen fallen, die häufig ein großes Aufsehen erregen und damit zur Steigerung des Bewusstseins für Phishing-Angriffe beitragen.

Die Schwächen einzelner Mitarbeiter durch ein gezieltes Spear-Phishing auszunutzen, birgt das Risiko, dass einer oder mehrere Mitarbeiter im Nachgang unzufrieden ist/ sind (siehe auch These 8). Beim Social Engineering werden menschliche Eigenschaften, wie die Hilfsbereitschaft (siehe Kapitel 6.7) verwendet. Eine professionell gemachte E-Mail, die keine Fehler beinhaltet, von einem bekannten und nachvollziehbaren Absender kommt und im richtigen Kontext gestellt wird, ist nur sehr schwer erkennbar. Die Erfolgsquote von Spear-Phishing kann als sehr hoch eingestuft werden, wie auch folgendes Zitat verdeutlicht:

> Spear-Phishing-E-Mails funktionieren, weil sie glaubhaft sind. 3 % der Spam-Nachrichten und 70 % der Spear-Phishing-E-Mails werden geöffnet. 50 % der Personen, die Spear-Phishing-E-Mails öffnen, klicken auch auf die Links darin (im Vergleich zu 5 % bei Massenmails), meist innerhalb einer Stunde nach Empfang. Bei einer Kampagne mit 10 E-Mails liegt die Wahrscheinlichkeit also bei 90 %, dass das Ziel in die Falle gelockt wird.[116]

Durch eine Spear-Phishing E-Mail ist quasi jeder Mensch angreifbar und dessen IT-System verwundbar. Dies durch ein Red Teaming zusätzlich zu testen und das Risiko der Unzufriedenheit der Mitarbeiter einzugehen, sollte kritisch hinterfragt werden.

Auch bei einem Physical Assessment ist ein auditbasiertes Assessment im ersten Schritt sinnvoller, bei dem in Abstimmung mit einem Auftraggeber Sicherheitsmaßnahmen der Infrastruktur überprüft werden. Die durch ein Audit verbesserten Maßnahmen durch ein unangekündigtes Red Teaming zu überprüfen, ist anschließend ein nachvollziehbarer Schritt.

---

[116] *FireEye*, Der beste Schutz vor Spear-Phishing-Angriffen..

6.2 Cyber Kill Chain

Es gibt viele unterschiedliche Angriffsmodelle. Diese können dabei helfen die Denk- und Vorgehensweise von Angreifern zu verstehen. In einem Red Teaming Projekt können diese Modelle nützlich sein, um ein Projekt zu strukturieren, die Prozesse darauf auszurichten oder die Kompetenzen auf unterschiedliche Köpfe zu verteilen.

Lockheed Martin ist ein globaler Security-, Luft- und Raufahrtkonzern, der hauptsächlich in den Bereichen Forschung, Design, Entwicklung, Herstellung, Integration und Wartung von Systemen, Produkten und Dienstleistungen tätig ist.[117] Die Organisation hat über einen längeren Zeitraum Angreifer überwacht und versucht, Muster zu erkennen. Auf dieser Basis wurde die Cyber Kill Chain entwickelt.

Das Cyber Kill Chain-Framework ist Teil des Intelligence Driven Defense-Modells zur Identifizierung und Prävention von Cyber-Angriffen. Das Modell beschreibt, was Angreifer durchführen müssen, um ihr Ziel zu erreichen. In der Abbildung 27: Lockheed Martin Kill Chain wird das Modell beschrieben.

[117] Vgl. *Lockheed Martin Corporation*, Lockheed Martin. Your Mission is Ours., 2019.

Abbildung 27: Lockheed Martin Kill Chain[118]

Das Modell kann als Grundlage für Red Teaming verwendet werden.

6.3 Expanded Cyber Kill Chain

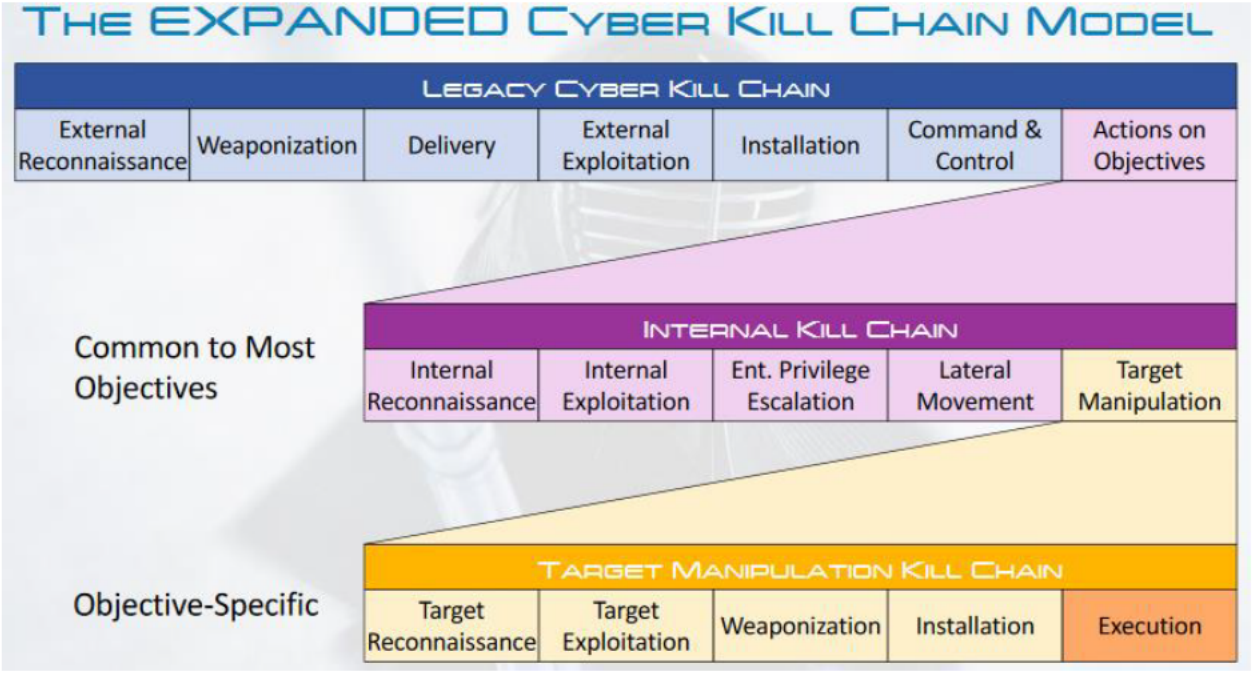
Das Cyber Kill Chain Modell bietet einen Rahmen, um zu verstehen, wie ein Gegner den Perimeter durchbricht, um Zugang zu Systemen im internen Netzwerk zu erhalten. Jedoch

[118] *Lockheed Martin Corporation*, The Cyber Kill Chain.

ist dieses Modell nach Expertenmeinungen unvollständig. Der primäre limitierende Faktor der traditionellen Cyber Kill Chain ist, dass diese mit Stufe 7 der „*Actions on objectives*“ endet. Dies vermittelt den Eindruck, dass, sobald der Gegner diese Phase erreicht hat und Zugang zu einem System im internen Netzwerk hat, das verteidigende Opfer bereits verloren hat. In Wirklichkeit sollte es mehrere Schichten von Sicherheitszonen im internen Netzwerk geben, um die kritischsten Vermögenswerte zu schützen. Der Gegner muss oft zahlreiche zusätzliche Phasen durchlaufen, um auf bestimmte Systeme zugreifen und diese manipulieren zu können und um sein Ziel zu erreichen. Aus diesem Grund wurde auf der Black Hat Konferenz die Expanded Cyber Kill Chain präsentiert.

Dieses erweiterte Modell beinhaltet zusätzlich zur bisherigen Cyber Kill Chain die Internal Kill Chain und die Target Manipulation Kill Chain unter der Phase „*Actions on Objectives*“. In diesen Modellen wird überprüft, welche Maßnahmen in jeder Phase ergriffen werden und was notwendig ist, damit der Gegner von einer Phase zur nächsten übergeht. In der folgenden Abbildung und den Tabellen wird die erweiterte Kill Chain beschrieben.[119]

Abbildung 28: Expanded Cyber Kill Chain Model



In den folgenden Tabellen wird die Internal Kill Chain und Target Manipulation Kill Chain erläutert.

Tabelle 23: Internal Kill Chain

Prozess	Ziele
Internal Reconnaissance	Data Mining verfügbarer Systeme und Abbildung des internen Netzwerks und der Schwachstellen erstellen.

[119] Vgl. *Malone, S. T.*, Using an expanded Cyber Kill Chain Model to increase attack resiliency, 2018.

Prozess	Ziele
Internal Exploitation	Ausnutzen von Informationen und Schwachstellen auf einem internen System.
Enterprise Privilege Escalation	In diesem Prozess werden kompromittierte Konten und Vertrauensbeziehungen genutzt, um höhere Berechtigungen zu erhalten.
Lateral Movement	Das Ziel ist es von einem Ausgangspunkt über kompromittierte Systeme in eingeschränkte Netzwerkzonen zu gelangen.

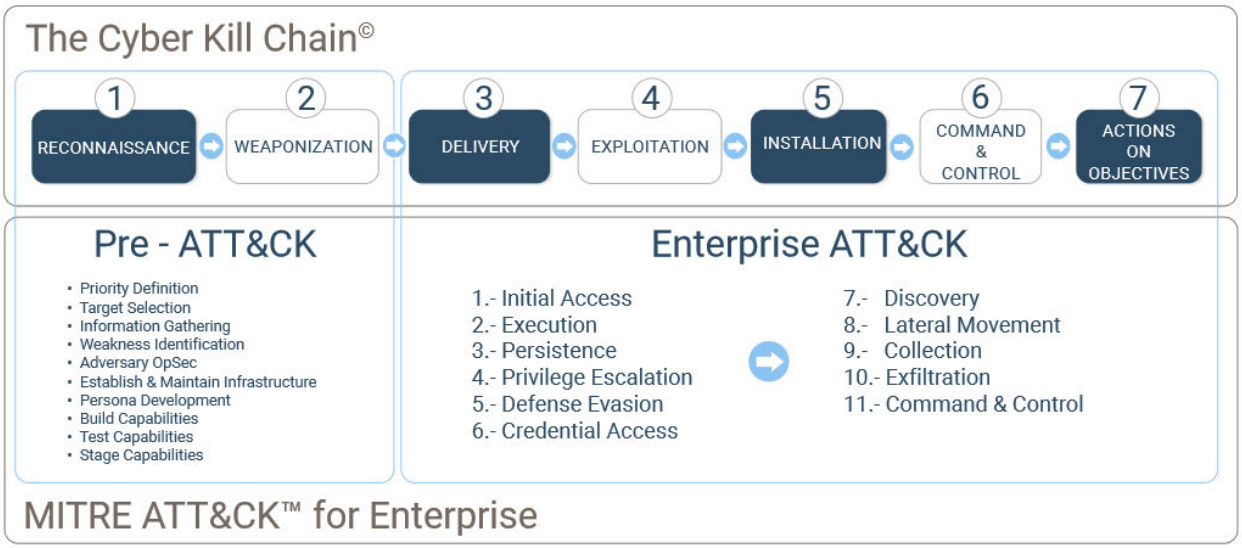
Tabelle 24: Target Manipulation Kill Chain

Prozess	Ziele
Target Reconnaissance	Es werden zielspezifische Systeme abgebildet und verstanden.
Target Exploitation	Zugriffe auf einem Zielsystem über Vertrauensbeziehungen oder neue Schwachstellen erhalten.
Weaponization	Entwicklung plattformspezifischer Malware für ein Zielsystem oder einen Geschäftsprozess.
Installation	Bereitstellung von benutzerdefinierter Malware auf dem Zielsystem.
Execution	Aktivieren der Malware auf dem Betrieb des Zielsystems mit den daraus resultierenden Folgen.

6.4 ATT&CK Framework

Ein alternatives Modell, das den Ablauf bei einem Angriff neben der Cyber Kill Chain (siehe Kapitel 6.2) beschreibt, ist das MITRE ATT&CK Framework und die darin beinhaltende ATT&CK-Matrix. Das ATT&CK-Framework hat eine wesentlich höhere Detailstufe wie die Kill Chain. Es ist vor allem dann hilfreich, wenn detailliert bestimmte APTs oder Angriffe analysiert oder nachgebildet werden sollen. Ein Vergleich der Frameworks wird in der folgenden Abbildung ersichtlich.

Abbildung 29: Vergleich Cyber Kill Chain und MITRE ATT&CK for Enterprise[120]



Das Massachusetts Institute Of Technology Research And Engineering (MITRE) bietet im ATT&CK Framework eine Wissensdatenbank über gegnerische Taktiken und Techniken, die auf realen Beobachtungen basiert. Diese sind als Matrix visualisiert. Diese kann als Grundlage für die Entwicklung spezifischer Bedrohungsmodelle und -methoden dienen.[121] Durch die ausführlich beschriebenen Taktiken und Techniken ist es ein ideales Nachschlagewerk für das Red und Blue Team bei Threat-/ APT-basierten Red Teaming Projekten.

Die ATT&CK Matrix ist in die Technologie-Domains Enterprise und Mobile unterteilt. Unter Enterprise wurden die Plattformen Windows, Linux und MacOS festgelegt und unter Mobile Android und iOS. Die ATT&CK-Matrix besteht aus einem Enterprise- und dem Pre-ATT&CK (siehe Abbildung 29: Vergleich Cyber Kill Chain und MITRE ATT&CK for Enterprise). Die Pre-ATT&CK Phase umfasst die Anforderungserfassung (engl. requirement gathering), die Aufklärung (engl. reconnaissance) und die Bewaffnung (engl. weaponization). Die Pre-ATT&CK Matrix ist Technologie-Unabhängig und versucht, einen Angreifer zu modellieren, der versucht, einen Zugang zu einem Unternehmen oder einer Organisation durch die Technologie, die diese einsetzt, zu erhalten. Die Matrix visualisiert den Zusammenhang zwischen Taktiken und Techniken. In den Spaltenüberschriften stehen die Taktiken und in den darunter liegenden Zellen die Techniken.[122]

Die Taktiken stellen das Warum einer Angriffstechnik dar. Es ist das taktische Ziel des Angreifers bei der Durchführung einer Aktion und dient als nützliche Kategorie für einzelne Techniken und deckt diese übergeordnet ab. In der Matrix werden folgende Taktiken abgebildet:

---

[120] *Cyber Startup Observatory*, The MITRE ATT&CK for Enterprise and the Cyber Kill Chain.
[121] Vgl. *MITRE*, MITRE ATT&CK™, 2019.
[122] Vgl. *Storm, B. E.* u. a., MITRE ATT&CK™: Design and Philosophy, 2018, S. 3, 6-7.

Abbildung 30: ATT&CK-Taktiken

ID	Taktik
TA0001	Initial Access
TA0002	Execution
TA0003	Persistence
TA0004	Privilege Escalation
TA0005	Defense Evasion
TA0006	Credential Access
TA0007	Discovery
TA0008	Lateral Movement
TA0009	Collection
TA0010	Exfiltration
TA0011	Command and Control

Die Techniken stellen dar, wie und was ein Angreifer macht, um ein taktisches Ziel zu erreichen. Es kann viele Möglichkeiten oder Techniken geben, um taktische Ziele zu erreichen, sodass es in jeder Taktikkategorie mehrere Techniken gibt. In der folgenden Tabelle sind die Techniken des initialen Zugangs (engl. Initial Access) aufgelistet. Eine Technik kann auf eine oder mehrere Plattformen angewendet werden.

Abbildung 31: ATT&CK-Techniken Initial Access

TA0001 Initial Access	
T1189	Drive-by Compromise
T1190	Exploit Public-Facing Application
T1200	Hardware Additions
T1091	Replication Through Removable Media
T1193	Spearphishing Attachment
T1192	Spearphishing Link
T1194	Spearphishing via Service
T1195	Supply Chain Compromise
T1199	Trusted Relationship
T1078	Valid Accounts

Neben den Techniken gibt es beim ATT&CK Framework Gruppen (engl. Groups). Dies sind mehrere Eindringungsaktivitäten, für die ein Name festgelegt wurde. Die Gruppen sind den angewendeten Taktiken und Techniken in der Matrix zugeordnet. Zu den Gruppen sind Softwares zugeordnet, die bei dem Angriff verwendet werden.

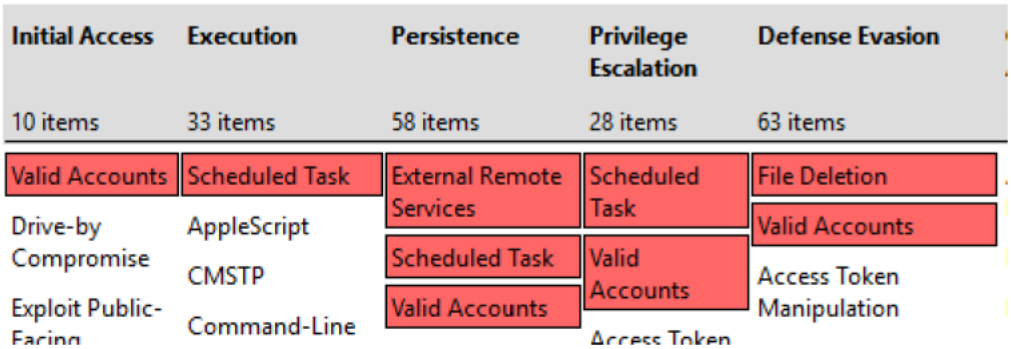
Abbildung 32: ATT&CK-Gruppe APT18

Gruppe	APT18
Beschreibung	APT18 ist eine Bedrohungsgruppe, die seit mindestens 2009 besteht und sich an eine Reihe von Branchen wie Technologie, Fertigung, Regierung und Medizin richten.
Alias	Dynamite Panda, Threat Group TG-0416
Techniques	T1133 External Remote Service

Gruppe	APT18
	T1107 File Deletion T1053 Scheduled Task T1078 Valid Accounts
Software	S0106 cmd S0032 gh0st S0071 hcdLoader S0070 HTTPBrowser S0124 Pisloader

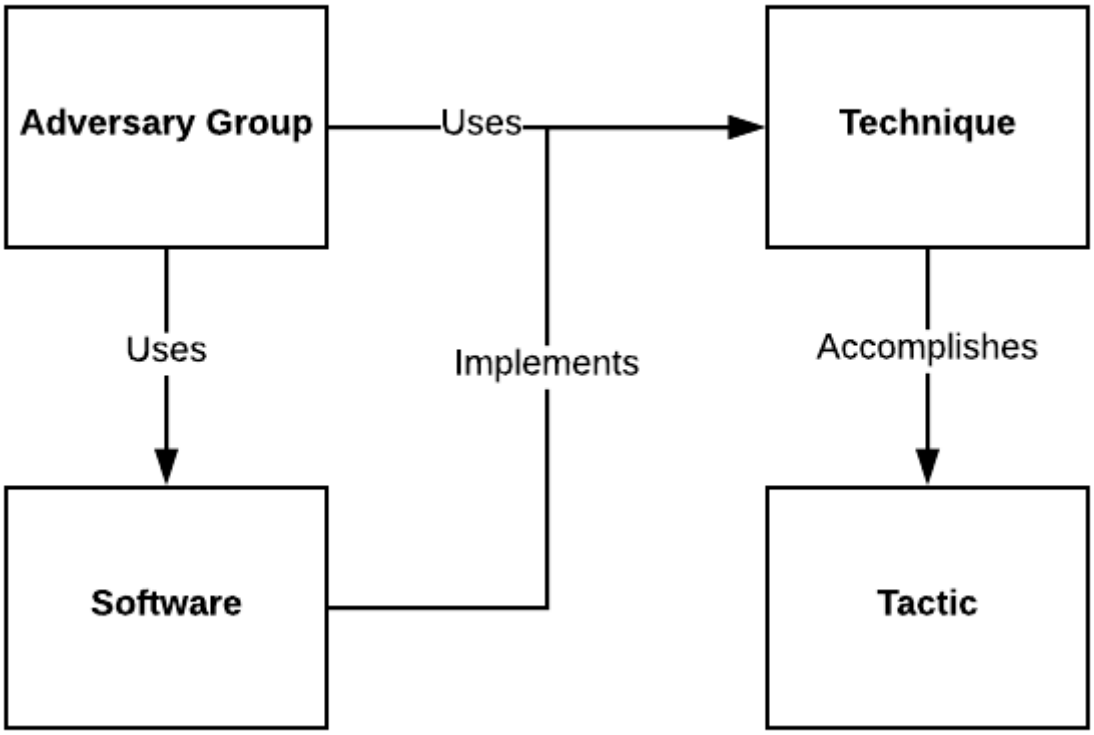
Auf Grundlage der Informationen können in der ATT&CK Matrix die Techniken markiert und die Taktiken identifiziert werden. Die Matrix kann mit dem ATT&CK Navigator visualisiert werden (siehe Abbildung 33: ATT&CK-Matrix APT18).

Abbildung 33: ATT&CK-Matrix APT18



Die Zusammenhänge können mit folgendem Modell beschrieben werden (siehe Abbildung 34: ATT&CK Modell). Angreifer-Gruppen (engl. adversary group) benutzen Techniken und Software, um ein taktisches Ziel zu erreichen. Die Software wird dazu verwendet, eine Technik zu implementieren.

Abbildung 34: ATT&CK Modell[123]



6.5 Unified Kill Chain

Um eine strukturierte Analyse von APTs durchzuführen, wurden die bereits beschriebene Cyber Kill Chain von Lockheed Martin und MITRE ATT&CK Framework entwickelt (siehe Kapitel 6.2 und Kapitel 6.4). Die Cyber Kill Chain ist ein branchenübliches Standardmodell zur Verteidigung von APTs. Dem Modell wird von Kritikern unterstellt, dass es zu sehr auf APTs und Malware fokussiert ist.[124] Zudem ist die Cyber Kill Chain bspw. nicht für Insider-Bedrohungen geeignet. Diese Problematik wurde auch im Kapitel 6.3 angesprochen, wodurch die Cyber Kill Chain erweitert wurde.

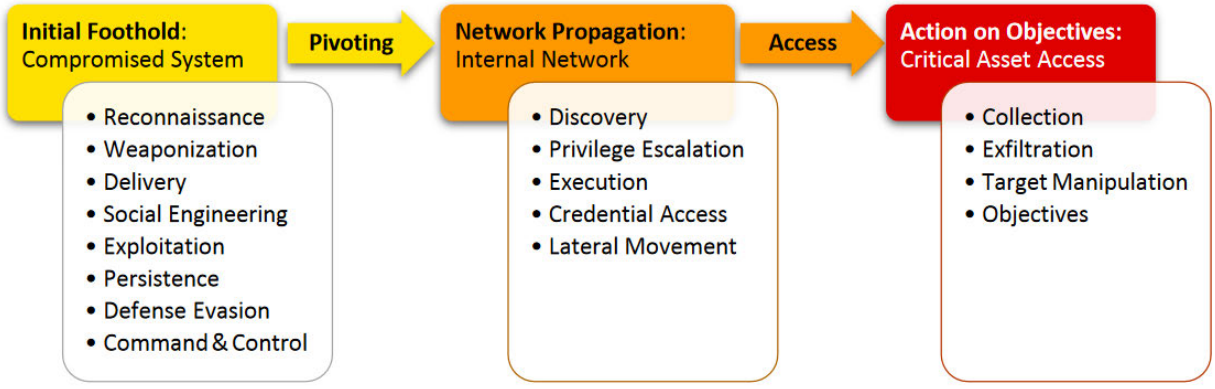
Ein Student der Cyber Security Academy hat aus diesem Grund eine Thesis verfasst, in der eine Unified Kill Chain entwickelt wurde. Die Unified Kill Chain ist eine Kombination aus der Cyber Kill Chain und dem ATT&CK Framework (siehe Abbildung 35: Unified Kill Chain). Sie wurde auf Basis mehrerer Modelle und Fallstudien entwickelt. [125]

Die Unified Kill Chain ist ein Angriffsmodell, das von Verteidigern und Red Teams genutzt werden kann, um neue und bestehende Verteidigungsstrategien zu entwickeln. In der

[123] *Knight, A.*, ATT&CK Model - Data Driven Investor - Medium, 2019.
[124] Vgl. *Engel, G.*, Deconstructing The Cyber Kill Chain, 2014.
[125] Vgl. *Bratović, I.*, MITRE ATT&CK and the Unified Kill Chain, 2019.

zukünftigen Forschung könnte durch die Unified Kill Chain eine breite Palette von Cyberangriffen verschiedener Bedrohungsakteure evaluiert und möglicherweise weiter verfeinert werden. Zusätzliche Fallstudien könnten das Unified Kill Chain validieren oder möglicherweise zusätzliche Taktiken identifizieren, die integriert werden könnten.[126]

Abbildung 35: Unified Kill Chain[127]



6.6 Prozessuale Durchführung

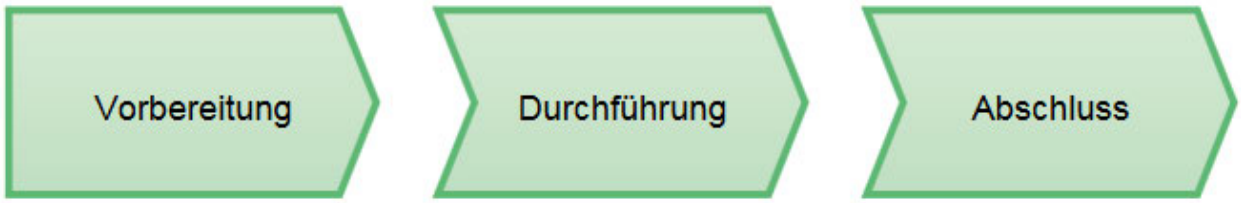
Wie im vorherigen Kapitel beschrieben ist es durchaus sinnvoll ein Red Teaming in einem Unternehmen durchzuführen, um die Erkennung und Reaktion auf Sicherheitsvorfälle zu verbessern. Aufgrund der vielen Ausprägungen, die in einem Red Teaming Projekt möglich sind, ist es nicht möglich den einen methodisch richtigen Weg zu beschreiben. In den folgenden Kapiteln soll vielmehr ein Prozess beschrieben werden, der für viele Red Teaming Projekte anwendbar und anpassbar ist. Die Basis des Prozesses sind die aus den theoretischen Grundlagen und Gesprächen erarbeitetes Wissen.

Bei der Umsetzung richten sich manche Dienstleister nach Frameworks wie dem TIBER-EU oder CBEST Framework. Sowohl CBEST als auch TIBER-EU sind für den Finanzsektor ausgelegt, können aber auf andere Branchen adaptiert werden. Ein Framework gibt nur die Rahmenstruktur vor. In diesem Kapitel soll die prozessuale und technische Umsetzung beschrieben werden, die nicht auf eine bestimmte Branche oder Ausprägung ausgelegt ist.

Aus dem Interview und den Recherchen ging hervor, dass Red Teaming, wie im TIBER-EU beschrieben (siehe Kapitel 2.10.5), in die drei übergeordnete Phasen Vorbereitung, Durchführung und Abschluss eingeteilt werden kann. Die Phasen werden in der Prozesslandkarte in der Abbildung 36: Phasen Red Teaming dargestellt und werden in den folgenden Kapiteln beschrieben.

[126] Vgl. *Pols, P.*, The Unified Kill Chain, 2017.
[127] *Pols, P.*, The Unified Kill Chain, 2017., S. 1.

Abbildung 36: Phasen Red Teaming



Der Prozess ist für beide Ausprägungen durchführbar.

6.6.1 Vorbereitung

Der Prozess wird von den Rollen Auftraggeber und dem Red Team begleitet (siehe Abbildung 37: EPK Vorbereitung). Beim Auftraggeber wird auch vom White Team gesprochen, das über den Test seitens des Auftraggebers informiert ist. Im ersten Schritt muss geprüft werden, ob Red Teaming die richtige Methodik für die angestrebten Ziele ist (siehe auch Kapitel 5 Methodik zur Einordnung der Prüfmethoden). Hierbei kann es hilfreich sein, sich mit einem Dienstleister abzustimmen, der sich mit unterschiedlichen Methodiken auskennt.

Wenn die Entscheidung auf Red Teaming fällt, muss ein Red Team ausgewählt werden. Dies ist bei Projekten in der Regel ein externer Dienstleister, der darauf spezialisiert ist. Es kann aber auch ein Team in einem Unternehmen engagiert werden. Wenn ein externer Dienstleister beauftragt wird, sollte dieser nach einem Auswahlverfahren mit festgelegten Kriterien ausgewählt und miteinander verglichen werden. Hierzu empfiehlt sich mehrere Angebote einzuholen, Vorgespräche mit den Anbietern zu führen, sich die Meinung Dritter einzuholen und, falls möglich, mit Referenzkunden zu sprechen.

> Das „Red Team“ sollte aus qualifizierten Prüfern bestehen, welche die Bereiche Systemadministration, Netzwerkprotokolle, IT-Sicherheitsprotokolle, Anwendungssysteme und Netzkomponenten beherrschen. Zudem sollten mehrere Programmiersprachen bekannt sein. Je mehr technische Kenntnisse und Erfahrungen in dem Team versammelt sind, desto erfolgreicher kann der simulierte Angriff ablaufen und mögliche langfristige Schäden, wie beispielweise das Ausfallen bestimmter angegriffener Systeme, können verhindert werden. Das „Red Team“ sollte neben den technischen Kenntnissen weitere Fähigkeiten, wie zielorientiertes Denken und Handeln, Überzeugungsfähigkeit, eine schnelle Auffassungsgabe und ein gesundes Urteilsvermögen besitzen. Schließlich sind diese Prüfer die Angreifer, die ihr Bestes geben werden, um in Ihre Systeme einzudringen. Auch sollte sich das „Red Team“ selbst organisieren können, es sollte analytisch die Infrastruktur begutachten können und im Team gemeinsam den Belastungen gewachsen sein, um insbesondere bei heiklen Sachverhalten zielorientiert arbeiten zu können. Das BSI empfiehlt, bei einer Überprüfung der IT-Sicherheit, Teams aus mindestens zwei Personen einzusetzen, damit das Vier-Augen-Prinzip gewahrt bleibt. Dabei spielt die Neutralität und Unabhängigkeit der Prüfer eine große Rolle. Steht einer der Prüfer in einem Abhängigkeitsverhältnis zu der getesteten Institution, fehlt die unerlässliche Unabhängigkeit, die für die Durchführung eines solchen Tests notwendig ist.[128]

Die Qualität der Ergebnisse ist maßgeblich von der Vorgehensweise, Erfahrung, Qualifikation und Wissen des Testteams abhängig. Daher ist es zu empfehlen den Anbieter

[128] *intersoft consulting services AG*, Cybersecurity – Red Team vs. Blue Team, 2019.

sorgfältig auszuwählen. Im TIBER-EU Framework werden Anforderungen an Red Team Dienstleister gestellt, die im Rahmen einer Auswahl hilfreich sein können.[129]

Wenn bereits ein oder mehrere Red Teaming Assessments von einem Red Team durchgeführt wurden, kann es auch sinnvoll sein, dieses zu wechseln, um so durch eine andere Vorgehensweise und Erfahrung einen anderen Einblick zu erhalten. Das Blue Team bilden häufig Mitarbeiter eines SOC oder IT-Mitarbeiter, die sich mit der Erkennung von Angriffen und Incident Response auseinandersetzen. Diese müssen vor einem Test nicht bestimmt und informiert werden. Es gibt aber auch Konstellationen, bei der ein Dienstleister das Blue Team unterstützt. Dies kann sinnvoll sein, um das Blue Team effizienter zu trainieren. Dies entspricht nicht dem klassischen Red Teaming Ansatz, sondern einem Purple Teaming.

Um die Rahmenbedingungen festzulegen, ist es empfehlenswert, einem Workshop zusammen mit dem beauftragten Red Team durchzuführen. In diesem Workshop können bspw. folgende Fragestellungen behandelt und erörtert werden:

- Was soll durch das Red Teaming erreicht werden?
- Was ist das Ziel vom Red Teaming?
- Was ist das Schlimmste, was einem Unternehmen passieren kann?
- Was tut dem Unternehmen besonders weh?
- Welche „Kronjuwelen“ bzw. sensiblen Informationen besitzt das Unternehmen?
- Welches Ziel soll erreicht werden?
- Welches sind die besonders schützenswerten Informationen?
- Was sind die kritischen Geschäftsprozesse und Funktionen im Unternehmen?
- Welche Bedrohungen hat das Unternehmen?
- Was darf im Test gemacht werden und was nicht?
- Was entspricht einem realen Angriff?
- Wann und wie oft erfolgt die Kommunikation im Testdurchlauf?
- Welche Risiken entstehen durch den Test?
- Wie ist der Ablauf des Projekts?
- Wie viel Zeit und Kosten werden für das Projekt investiert, bzw. was ist ein vertretbarer Umfang?

Die aufgeführten Fragen haben keinen Anspruch auf Vollständigkeit und sollen vielmehr als Ideen dienen. Ein Dienstleister sollte zur Vorbereitung eines Workshops einen Fragenkatalog vorbereiten und der Auftraggeber sich mit derartigen Fragen auseinandersetzen. Es ist ratsam, sich für einen solchen Workshop bereits die notwendigen Informationen zurecht zu legen, um effizient zu einem Ergebnis zu kommen. Anhand des durchgeführten Workshops kann ein Vertrag mit allen vereinbarten Rahmenbedingungen erstellt werden. Ein Vertrag kann durch ein Geheimhaltungsvertrag (engl. NDA; non-

[129] Vgl. *ECB*, ECB publishes European framework for testing financial sector resilience to cyber attacks, 2018., S. 20.

disclosure agreement) ergänzt werden. Zudem muss in einem Projektmanagement das Projekt geplant werden. Diese Dokumente müssen vor der Durchführung abgestimmt sein.

> Beim Planen und Durchführen eines Angriffs darf man zu keinem Zeitpunkt aus den Augen verlieren, dass in den meisten Fällen nicht nur das Unternehmen selbst betroffen ist, sondern auch dessen Mitarbeiter oder Kunden als natürliche Personen – mitsamt ihren personenbezogenen Daten. Für Mitarbeiter trifft das beispielsweise zu, wenn Social Engineering-Techniken eingesetzt werden, um an Login-Daten zu gelangen. Erfahrene Red Teamer lassen daher die Planung des Angriffes juristisch begleiten und binden, sobald Mitarbeiter betroffen sein können, von Anfang an die jeweilige Mitarbeitervertretung ein. (...) Nur so können die Mitbestimmungsrechte der Mitarbeiter gewahrt werden und das Unternehmen hat nicht zu befürchten, dass zwar der Test selbst erfolgreich ist, im Anschluss aber die Mitarbeiter juristisch gegen das Unternehmen vorgehen, da ihre Rechte verletzt wurden. Gerade um die Billigung des Tests durch eine Mitarbeitervertretung zu erlangen, empfiehlt es sich, ein nachweislich erfahrenes Unternehmen zu beauftragen, denn dieses kennt die üblichen Vorbehalte und ist in der Lage, Red Team Assessments betriebs- oder personalratskonform auszuführen.[130]

Weitere Informationen zu den rechtlichen Rahmenbedingungen wurden in Kapitel 5 betrachtet.

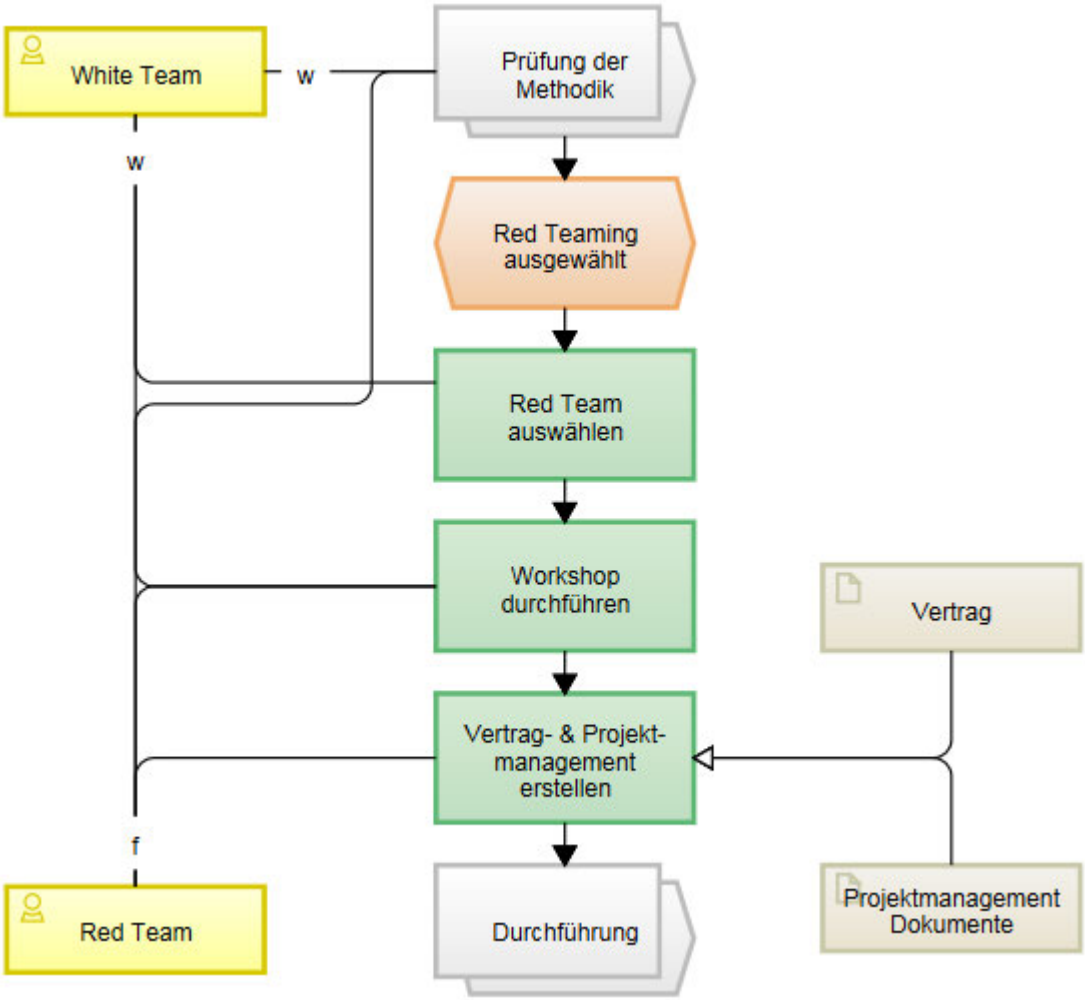
Die Phase Vorbereitung wird als ereignisgesteuerte Prozesskette (EPK) dargestellt (siehe Abbildung 37: EPK Vorbereitung). Triviale Ereignisse, bspw. dass eine Funktion abgeschlossen ist, wurden weggelassen. Die Kurzbezeichnungen können aus folgender Legende Tabelle 25: Legende Prozessdiagramme abgelesen werden.

Tabelle 25: Legende Prozessdiagramme

Abkürzung	Bezeichnung
w	wirkt mit
f	führt aus
e	entscheidet

[130] *IX-REDAKTION*, iX Kompakt (2019) IT-Sicherheit., S. 95.

Abbildung 37: EPK Vorbereitung



6.6.2 Durchführung

Allgemein kann für die Durchführung des Red Teaming die Cyber Kill Chain als Grundlage verwendet werden. Die Cyber Kill Chain ist ein mehrstufiges Modell, das vom Militär auf die Cyber-Sicherheit übertragen wurde. Mit diesem Modell werden Angriffe strukturiert und in einzelne Schritte zerlegt.[131] Es kann zur Grundlage für die Dokumentation oder den Phasen im Projektmanagement dienen. Weitere Informationen wurden bereits in Kapitel 6.2 beschrieben.

Der gesamte Prozess der Durchführung wird vom Red Team begleitet. Hierzu ist es sinnvoll, dass der komplette Ablauf detailliert dokumentiert wird. Die einzelnen Prozessschritte im Projektmanagement oder dem Ergebnisbericht könnte bspw. nach den Phasen der Cyber Kill Chain gegliedert werden. Dies dient für die spätere Nachvollziehbarkeit und den abschließenden Ergebnisbericht, sowie der Kommunikation mit dem White oder Blue Team. Die Cyber Kill Chain ist als ein lineares Modell dargestellt, doch kann es zwischen den Schritten zu Rücksprüngen kommen. Der Durchgang der einzelnen Schritte entspricht somit

[131] Vgl. *Schonschek, O./Schmitz, P.*, Cyber Kill Chain - Grundlagen, Anwendung und Entwicklung, 2017.

eher einer Schleife oder Spirale, welche durchlaufen wird, bis ein Ziel erreicht ist. Ein Grund für einen Rücksprung kann bspw. sein, wenn ein Angriff durch das Blue Team erkannt wird oder mehrere Angriffswege durchgeführt werden. Jeder Prozess kann dadurch auch mehrmals in einem Projekt durchlaufen werden.

Bei der Reconnaissance (dt. Aufklärung) sucht der Tester nach Angriffswegen, indem Informationen über die Zielorganisation gesammelt werden. In dieser Phase kann ein Open Source Intelligence (OSINT) und/oder ein Threat Intelligence (TI) durchgeführt werden. OSINT und TI schließen sich nicht gegeneinander aus. Die EZB beschreibt im TIBER-EU Framework eine optionale Phase, bei der eine Bedrohungslandschaft (Genereic Threat Landscape (GTL)) erstellt wird (siehe Kapitel 2.10.5). Wenn ein Auftraggeber gezielt auf bestimmte APT bzw. Bedrohungen prüfen möchte, ist es empfehlenswert, eine GTL zu erstellen oder die Informationen von öffentlich verfügbaren Reports oder TI Abteilungen zu betrachten.

Aus den Gesprächen mit den Dienstleistern ging hervor, dass nicht bei jedem Red Teaming eine TI verwendet wird bzw. die Bedrohungslandschaft analysiert wird. Dies wird begründet, da sich Angriffe ständig verändern und weiterentwickeln, sowie Reports auf Vergangenheitswerten beruhen. Daher stützen diese Dienstleister bevorzugt die Angriffe auf Grundlage der Informationen aus dem OSINT und eigenen Erfahrungen.

Nach der Aufklärung folgt die Weaponization (dt. Bewaffnung). Hier geht es darum, die passenden Angriffswerkzeuge vorzubereiten, z. B. einen Exploit erstellen oder eine Domain für eine Phishing-Webseite vorzubereiten. Diese Phase ist abhängig von den gefundenen Informationen der vorherigen Phase und den vereinbarten Angriffswegen.

Im Delivery-Prozess (dt. Zustellung) startet der Angriff. Dieser ist abhängig von den Informationen aus dem OSINT, der TI und den vorbereiteten Waffen. Die Zustellung kann auch auf physischem Weg bspw. durch Einbringen eines Netzwerkimplantats in ein Unternehmen erfolgen. Dies ist ein sehr kleiner Computer, über den eine Verbindung von außen ins Netzwerk aufgebaut werden kann.

Anschließend kommt es zum Exploiting (dt. Ausnutzung) der Schwachstelle. In dieser Phase ist tlw. das Mitwirken des angegriffenen Nutzers erforderlich, z. B. bei einem Phishing-Angriff bei dem der Nutzer auf einen Link oder einen Anhang klicken muss, um diesen auszuführen. Bei technischen Angriffen kann eine Schwachstelle auch ohne eine Benutzerinteraktion ausgeführt werden. Sobald der Tester einen Weg zum Ziel gefunden hat, versucht er sich durch eine Installation zu persistieren. Eine Persistenz kann durch das Einrichten eins Backdoors oder das Ausführen einer Malware erreicht werden.

Im Prozess Command & Control (dt. Kommandieren und Kontrollieren) wird der eingebrachte Zugangspunkt von außen gesteuert, um ein Ziel zu erreichen.

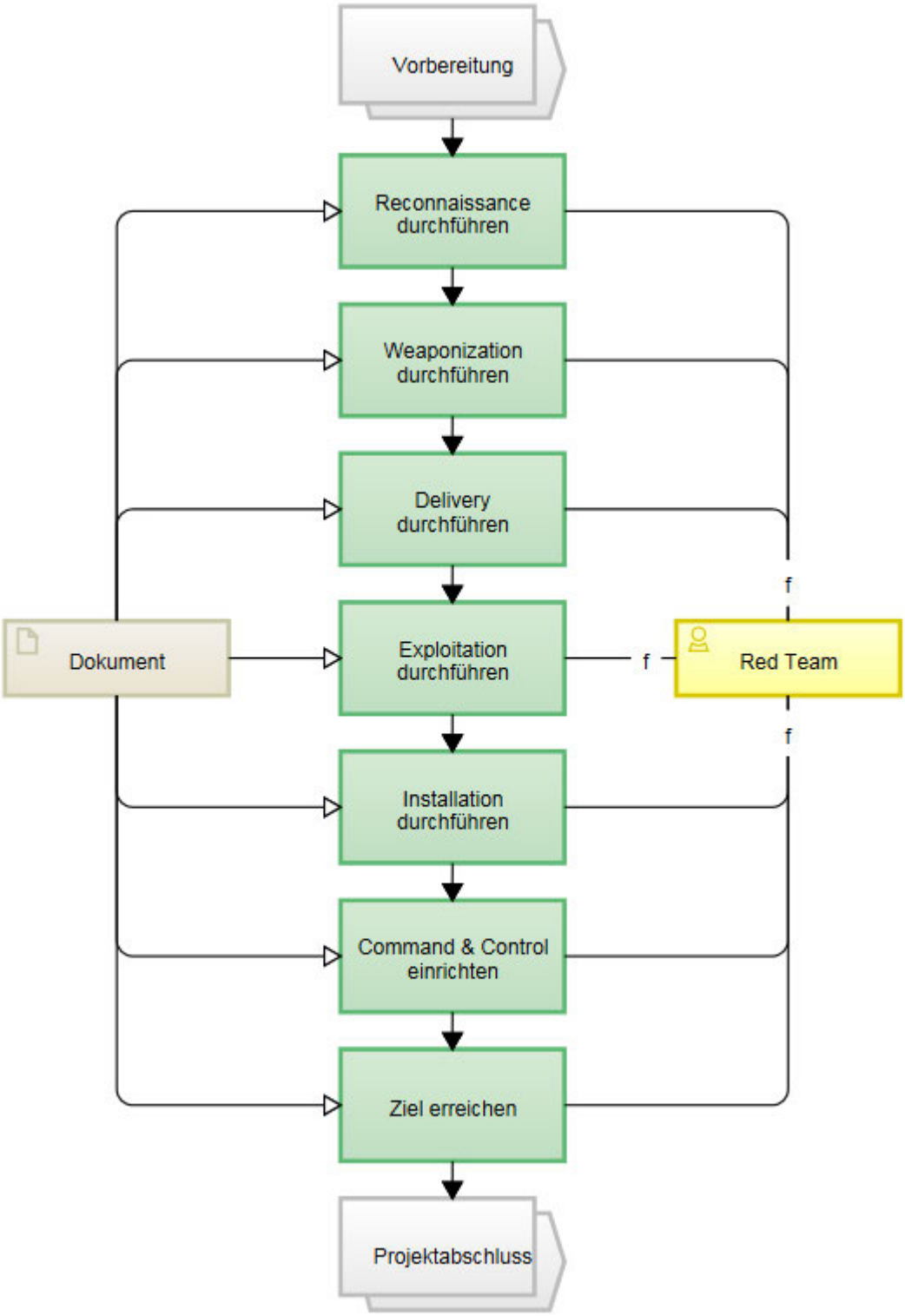
Die letzte Phase in der Kill Chain wird als Actions on Objectives (dt. Maßnahmen zum Erreichen der Ziele) bezeichnet. In diesem Prozess geht es bspw. Darum, Rechte zu

erweitern, im Netzwerk auszubreiten, um letztendlich das vorgegeben Ziel zu erreichen. Bei einem physischen Angriff kann auch das Ziel sein, in einen bestimmten Bereich in ein Gebäude zu kommen und dort einen Beweis zu erbringen, dass das Red Team dort war.

Die Cyber Kill endet nicht in der Phase Actions on objectives, es sind stattdessen noch weitere Schritte notwendig, die in der Expanded Cyber Kill Chain beschrieben werden. Bei diesem Modell wird der Phase „*Actions on Objectives*“ eine „*Internal Kill Chain*“ und innerhalb von dieser eine „*Target Manipulation Kill Chain*“ ergänzt. Diese Ketten beschreiben den Ablauf innerhalb eines Netzwerks oder innerhalb eines Ziels (siehe Kapitel 6.3), um letztendlich ein vorgegebenes Ziel zu erreichen. Die Expanded Cyber Kill Chain ist Bestandteil der Cyber Kill Chain und wird daher in der Abbildung 38: EPK Durchführung nicht visualisiert. Eine weitere Möglichkeit ist es, die Unified Kill Chain von der Cyber Security Akademie zu verwenden. In diesem Modell wird das ATT&CK-Framework und die Cyber Kill Chain kombiniert (siehe Kapitel 6.4). Die Verwendung von der Expanded Cyber Kill Chain und der Unified Kill Chain ist abhängig davon, welcher Detailgrad benötigt wird.

Folgende Abbildung zeigt den Prozess der Durchführung als EPK visualisiert. Es wurde die Cyber Kill Chain verwendet, da dies ein branchenübliches Standardmodell ist und eine höhere Abstraktionsebene hat. Es ist somit auf viele Fälle anwendbar. Wer eine höhere Detailstufe benötigt, kann die Expanded Cyber Kill Chain oder die Unified Kill Chain verwenden.

Abbildung 38: EPK Durchführung



Das Blue Team wird vor einem Angriff nicht informiert und kann den Angriff nicht von einem realen Angriff unterscheiden. Zur Verteidigung kann ebenfalls die Cyber Kill Chain verwendet werden. Beispiele, was die Verteidigung machen kann, um Angriffe zu erkennen und darauf zu reagieren, wird in folgender Tabelle beschrieben.

Abbildung 39: Lockheed Martin Cyber Kill Chain[132]

Stufe	Verteidigung
Reconnaissance	- Minimierung öffentlich einsehbarer Informationen - Auswerten von Zugriffen auf Webseiten und Servern, um verdächtige Suchaktivitäten aufzudecken
Weaponization	- Suche nach Spuren von Angriffsversuchen, z. B. durch Log-Auswertungen - Analysieren von entdeckter Malware und Überprüfung typischer Einsatzzwecke
Delivery	- Überwachung möglicher Angriffswege - Analyse entdeckter Angriffe (IT-Forensik), um die Ziele und Absichten besser zu verstehen
Exploitation	- Beseitigung von Schwachstellen - Sensibilisierung von Nutzern
Installation	- Überprüfung von Installationen, Aktivitäten, Zertifikaten und Berechtigungen - Blockieren von verdächtigen Aktionen
Command & Control	- Malware-Aktivitäten untersuchen, um Kommunikationskanäle aufzuspüren und zu blockieren
Actions on objectives	- Suche nach verdächtigen Aktivitäten - Durchführung forensischer Analysen - Start des Notfallprogramms, um den Schaden einzudämmen

Für Unternehmen, die auf Grundlage von einer Bedrohungsanalyse Red Teaming durchführen, ist zu empfehlen, sich nach dem ATT&CK-Framework zu richten. Das Red Team kann das ATT&CK-Framework als Informationsquellen für Bedrohungsgruppen nutzen und deren TTPs finden. Auf dieser Basis können Angreifer bzw. Angriffe nachgestellt oder eigene Angriffe entwickelt werden. Weitere Informationen über das ATT&CK-Framework wurden in Kapitel 6.4 beschrieben. Die Idee dieser Arbeit ist, dass das Projekt nach der Cyber-Kill-Chain strukturiert wird, aber die Angriffe, wenn sie bspw. auf APTs beruhen, mit Hilfe des ATT&CK-Framework geplant werden.

Im Bericht zur Lage der IT-Sicherheit vom BSI wird eine Zuordnung von einem APT zu einer bestimmten Branche gemacht. In diesem Beispiel besteht eine Bedrohung von APT18 in den Branchen Energie, Finanzen und Telekommunikation.

[132] *Schonschek, O./Schmitz, P.*, Cyber Kill Chain - Grundlagen, Anwendung und Entwicklung, 2017.

Abbildung 40: Ausschnitt Zuordnung APT zur Branche[133]

Energie	Finanzen	Telko
APT10 APT18/ Wekby APT29/ CozyBear Charming- Kitten	APT18/ Wekby APT29/ CozyBear BlueMush- room Dark-	APT18/ Wekby Codoso Emissary- Panda Hammer- Panda

Branchenspezifische Bedrohungsdaten können auch von anderen Sicherheitsdienstleistern wie von Fireye ausgelesen werden.[134] Durch bekannte APTs und der Matrix von MITRE kann eine Zuordnung von einer APT zu einer Branche, zu eingesetzten Techniken und Taktiken und der eingesetzten Software erfolgen. Die Matrix ist somit ein nützliches Werkzeug, sowohl für das Red, als auch das Blue Team.[135] Es dient dazu, die Denkweise von Angreifern von bekannten Bedrohungen zu verstehen und anzuwenden, sowie Pläne zu erstellen und Angriffe zu organisieren. Diese werden von MITRE als Adversary Emulation Plans bezeichnet.[136]

Die Association of Banks in Singapur hat im November 2018 für den Finanzsektor ein Werk veröffentlicht, in dem der Red Teaming Prozess beschrieben wird. In diesem Leitfaden wird beschrieben, wie ein Threat Modelling Report aufgebaut werden kann. Der Threat Modelling Report beschreibt die Absicht (engl. intent) und Fähigkeiten (engl. capability) von Bedrohungsakteuren, die anhand einer Übersichtstabelle bewertet und eingestuft werden. Dieser Bericht kann genutzt werden, um Angriffsszenarien für das Red Teaming zu priorisieren.[137] Ein Beispiel kann der Abbildung 41: Bedrohungsmatrix und Abbildung 42: Bedrohungstabelle entnommen werden.

[133] Vgl. *BSI*, Die Lage der IT-Sicherheit in Deutschland 2018, 2018.
[134] Vgl. *FireEye*, Branchenspezifische Bedrohungsdaten.
[135] Vgl. *Storm, B.*, ATT&CK™, 2018.
[136] Vgl. *MITRE*, Adversary Emulation Plans.
[137] Vgl. *The Association of Banks in Singapore*, Red Team: Adversarial Attack Simulation Exercises, 2018., S. 37-39.

Abbildung 41: Bedrohungsmatrix

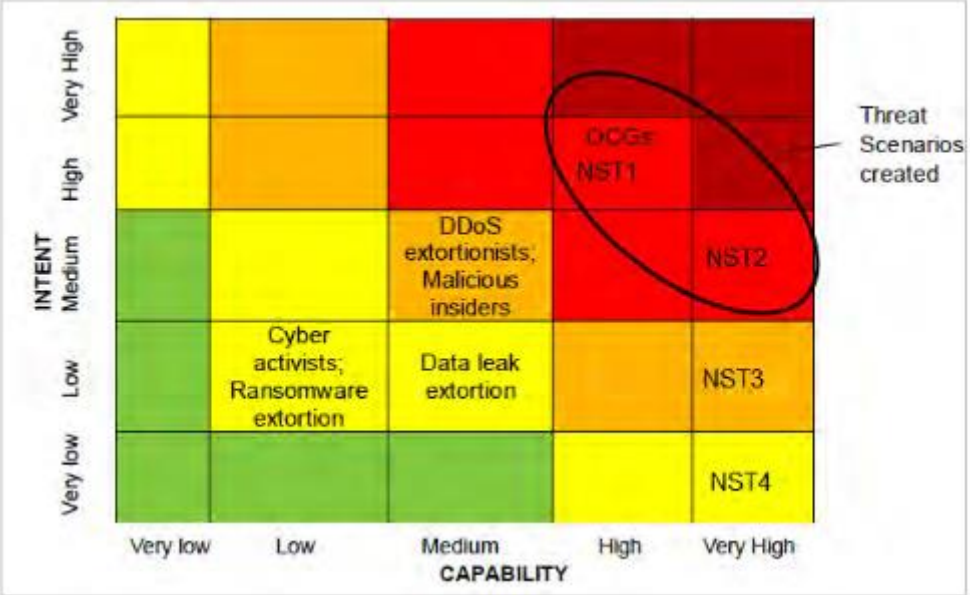


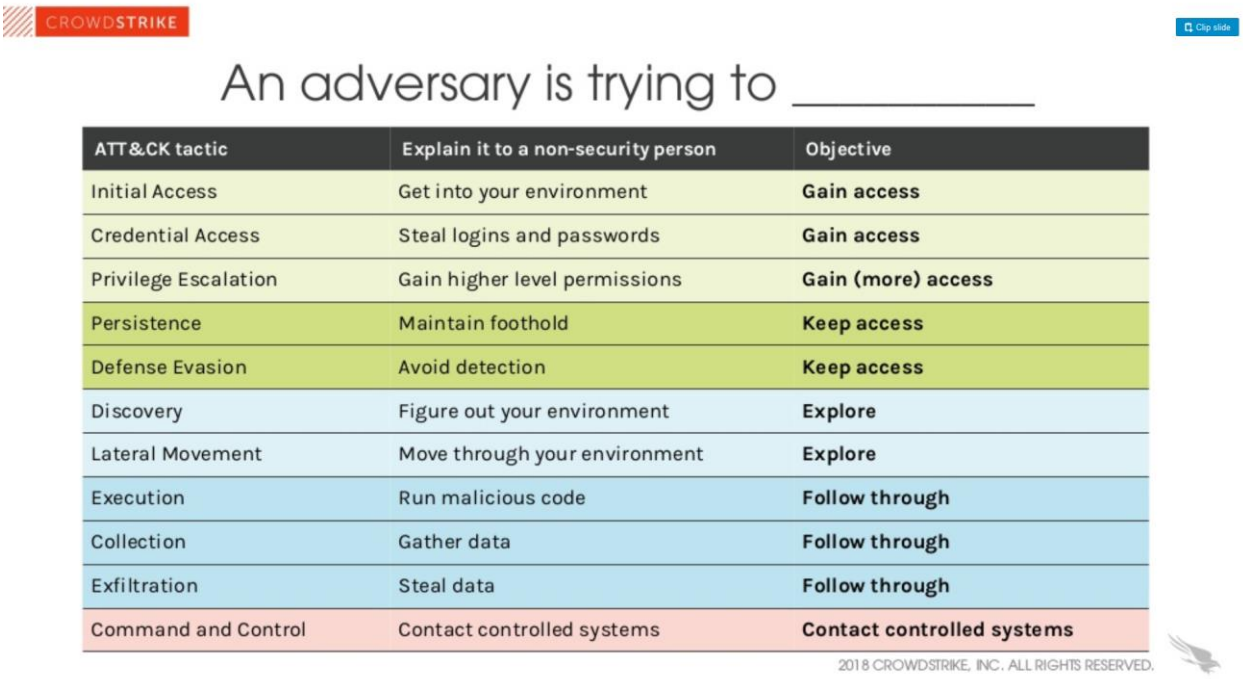
Abbildung 42: Bedrohungstabelle

Threat Actor	Intent	Capability	Threat	Summary
Organised cybercriminal groups (OCGs)	High	High	HIGH	OCGs are the most sophisticated of cybercriminal actors, and have demonstrated their capability to compromise various different types of systems in scope for this engagement. Although they have been more active in financial centres other than Country X, Organisation X will still likely represent an attractive target.

Neben dem Reporting ist die Kommunikation mit Personen, die nicht aus dem IT-Sicherheitsbereich kommen, sehr wichtig. Auf der ATT&CKcon wurde ein Ansatz präsentiert, wie das ATT&CK-Framework einer Interessengruppe, die nicht aus dem Sicherheitsbereich kommt, in zehn Minuten erklärt werden könnte.[138] Einen Auszug aus der Präsentation ist in der Abbildung 43: Erklärung ATT&CK-Taktiken abgebildet.

[138] *Searle, E.*, Helping Non-Security Stakeholders Understand ATT&CK in 10 Minutes or Less, 2019.

Abbildung 43: Erklärung ATT&CK-Taktiken

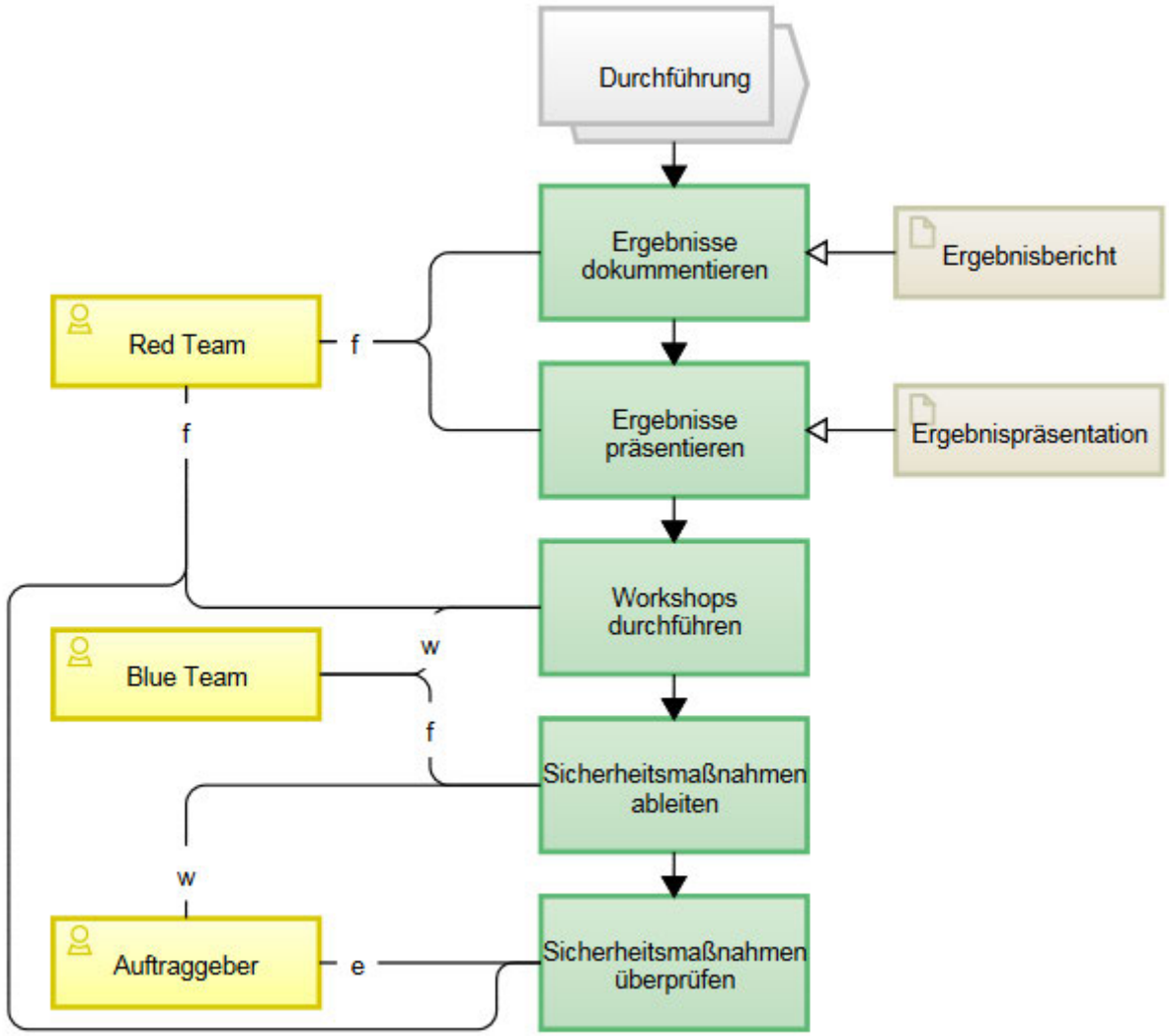


ATT&CK tactic	Explain it to a non-security person	Objective
Initial Access	Get into your environment	**Gain access**
Credential Access	Steal logins and passwords	**Gain access**
Privilege Escalation	Gain higher level permissions	**Gain (more) access**
Persistence	Maintain foothold	**Keep access**
Defense Evasion	Avoid detection	**Keep access**
Discovery	Figure out your environment	**Explore**
Lateral Movement	Move through your environment	**Explore**
Execution	Run malicious code	**Follow through**
Collection	Gather data	**Follow through**
Exfiltration	Steal data	**Follow through**
Command and Control	Contact controlled systems	**Contact controlled systems**

6.6.3 Abschluss

In der Abschluss Phase müssen alle Ergebnisse vom Red Team nachvollziehbar für den Auftraggeber und das Blue Team dokumentiert werden. Um eine strukturierte Vorgehensweise zu gewährleisten, bietet es sich an, eine Dokumentenvorlage zu erstellen. Bei den Ergebnissen sollten auch mögliche Sicherheitsmaßnahmen auf die genannten Schwachstellen oder Empfehlungen, wie ein Angriff erkannt oder darauf reagiert werden kann, gegeben werden. Bei Social Engineering Angriffen ist auf den Datenschutz zu achten (siehe auch Kapitel 3). Die Ergebnisse sollten dem Auftraggeber und dem Blue Team sowie ggf. noch weitere Beteiligten, wie Applikationsverantwortlichen, präsentiert werden. Anschließend kann es sinnvoll sein, Workshops mit dem Blue Team durchzuführen, um dieses zu trainieren und Verbesserungsmaßnahmen für die Erkennung- und Reaktion einzuleiten. Der Auftraggeber und das Blue Team sollten im Nachgang Sicherheitsmaßnahmen ableiten. Es ist auch zu empfehlen, eingeführte Maßnahmen erneut mit einem Red Team zu überprüfen. Nachdem die Sicherheitsmaßnahmen für die gefundenen Schwachstellen behoben und geprüft wurden, kann ein Red Teaming abgeschlossen und von neuem gestartet werden. Auch ein dauerhaft laufender Red Teaming Prozess ist denkbar, aber aufgrund des Aufwands und der Kosten für die meisten Unternehmen eher unrealistisch. Der Prozess Abschluss ist in folgender Abbildung visualisiert.

Abbildung 44: EPK Abschluss



6.6.4 Fazit

Der Red Teaming Prozess wurde in die drei Phasen Vorbereitung, Durchführung und Abschluss aufgeteilt. Die Prozesse der Phasen wurden in den Kapiteln beschrieben. In der Durchführung wurde die Cyber Kill Chain von Lockheed Martin als Grundlage verwendet. Wenn eine bedrohungsbasiertes Red Teaming durchgeführt wird, kann das MITRE ATT&CK-Framework hilfreich sein. Wenn eine höhere Detailstufe wie bei der Cyber Kill Chain benötigt wird, kann die Expanded Kill Chain oder die Unified Kill Chain verwendet werden.

6.7 Technische Umsetzung

Bisher wurde auf rein prozessualer Ebene die Umsetzung eines Red Teaming beschrieben. In den folgenden Kapiteln geht es darum welche Angriffe in einem Red Teaming gemacht werden können oder üblich sind. Hierzu wurde das Kapitel nach der personellen, physischen und technischen Sicherheit gegliedert. Die Beschreibungen sind abhängig vom jeweiligen Unternehmen und der Infrastruktur. In dieser Arbeit kann keine vollständige Liste von

Angriffsmöglichkeiten geliefert werden, sondern nur einige Beispiele, die in der Praxis Einsatz finden können.

6.7.1 Personelle Sicherheit

Zweck der personellen Sicherheit ist es, die Risiken, die durch menschliche Fehler, Diebstahl, Betrug und Missbrauch von Einrichtungen hervorgerufen werden, zu reduzieren. Zu den Angriffen auf die personelle Sicherheit gehört das Social Engineering.[139] Social Engineering ist eine Methode, bei der ein unberechtigter Zugang zu Informationen oder IT-Systemen erlangt werden soll, indem menschliche Eigenschaften wie z. B. Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autoritäten ausgenutzt werden. Dadurch werden Mitarbeiter so manipuliert, dass sie unzulässig handeln.[140] In einem Internetartikel werden die zehn beliebtesten Social-Engineering-Methoden 2019 auf Basis der McAfee Studie *Hacking the Human Operation System* präsentiert.[141] Die am häufigsten eingesetzte und effizienteste Variante, welche aus den Interviews und der Recherche (siehe Kapitel 2.4) hervorgeht, ist das (Spear-)Phishing. Mit einer gezielten E-Mail wird versucht, eine Person dazu zu bringen, einen angegebenen Link oder einen Anhang auszuführen, um sich mit einer präparierten Malware zu infizieren oder in einer manipulierten Webseite sensible Daten anzugeben. Hierzu wird von den Dienstleistern eine Malware vorbereitet oder eine Domain registriert und eine Phishing-Webseite aufgebaut. Die E-Mail wird so präpariert, dass es für ein Nutzer nur schwer oder unmöglich ist, ein Phishing zu erkennen. Beispielsweise wird eine manipulierte Anmeldeseite dazu verwendet, Zugangsdaten zu stehlen.

Das Tailgating wird verwendet, um auf physischen Weg in ein Gebäude zu kommen. Hier gibt sich der Tester bspw. als ein Dienstleister oder Lieferant des Unternehmens aus, um eine Zugangskontrolle zu überwinden. Durch Verkleidung, nachgemachte Ausweise, Kreditkarten und glaubwürdige Geschichten wird ein Empfangspersonal so getäuscht, dass dem Tester der Zutritt in das Gebäude gewährt wird. Aber nicht immer ist eine Täuschung notwendig, denn auch offene Türen oder ein Mitarbeiter, der die Tür offenhält, können als Eintrittsmöglichkeiten dienen. Weitere Informationen zur physischen Sicherheit werden in Kapitel 6.7.2 beschrieben.

Auch die Methode Pretexting, bei der eine glaubwürdige Geschichte erfunden wird, um an bestimmte Informationen zu kommen, ist gängige Praxis. Diese wird häufig in Kombination mit anderen Methoden eingesetzt, wie z. B. dem Phishing oder Tailgating. Als Basis für die Inhalte bei Social-Engineering Methoden werden die gewonnen Informationen aus öffentlichen Quellen der OSINT-Phase verwendet. Alle weiteren Methoden, die in der McAfee

[139] Vgl. *Kersten, H.* u. a., IT-Sicherheitsmanagement nach der neuen ISO 27001, 2016, S. 135.
[140] Vgl. *BSI*, BSI - G 5 Gefährdungskatalog Vorsätzliche Handlungen - IT-Grundschutz-Kataloge - G 5.42 Social Engineering..
[141] Vgl. *Laufenburger, R.*, Zehn beliebte Social-Engineering-Methoden im Überblick, 2019..

Studie beschrieben werden, können ebenfalls in einem Red Teaming eingesetzt werden. In der Befragung wurden diese aber eher selten oder gar nicht erwähnt.

Zur Vorbereitung von Social Engineering Angriffen kann es hilfreich sein, die psychologischen Hebel der Social Engineering-Angreifer zu betrachten und zu verwenden (siehe Abbildung 45: Psychologischer Hebel Social Engineering), um einen effektiven und glaubwürdigen Angriff durchführen zu können.[142]

[142] *Schonschek, O.*, Social Engineering – was Sie dazu wissen müssen, 2019.

Abbildung 45: Psychologischer Hebel Social Engineering

Psychologischer Hebel der Datendiebe	Beispiel
Methode „Herdentrieb": Alle machen dies, Du musst dies auch tun.	Angebliche E-Mail des Administrators: Alle anderen Mitarbeiter haben fristgerecht ihr Passwort geändert. Machen Sie dies nun auch (endlich)!
Methode „Autorität": Du musst gehorchen. Dabei werden auch entsprechende Logos und Bilder eingesetzt.	Angebliches Fax der Bank: Es gibt ein Problem mit einer Überweisung. Rufen Sie eine (gefälschte) Nummer an und wiederholen Sie den Zahlungsvorgang.
Methode „Attraktivität": Ich mag Dich, vertrau mir.	Angebliche E-Mail einer Verehrerin: Ich habe Dein Facebook-Profil gesehen und will Dich heiraten. Aber ich brauche Deine Hilfe …
Methode „Pflichtbewusstsein": Als guter Bürger musst Du dies tun.	Angeblicher Brief der Stadtverwaltung: Jeder Bürger muss auf Bankeinzug umstellen, faxen Sie uns die Bankverbindung mit diesem Formular.
Methode „Keine Zeit": Du musst sofort reagieren.	Angebliche Gewinnbenachrichtigung: Melden Sie sich sofort als Gewinner zurück, sonst ist es zu spät.
Methode „In der Schuld sein": Ich habe Dir geholfen, nun bist Du dran.	Angebliche Nachricht des Schulkameraden: Ich habe Dir in der Schule geholfen, jetzt brauche ich Deine Hilfe.
Methode „Drohung": Ich veröffentliche Vertrauliches über Dich.	Nachricht des Angreifers, dass er vertrauliche Daten über das Opfer verbreiten werde, wenn nicht dieses oder jenes getan wird (Online-Pressung).
Methode „Hilfsbereitschaft": Mache das, ich zeige Dir, wie es geht.	Nachricht des Angreifers, die eine genaue Anleitung und sogar eine FAQ-Liste enthält, die es dem Opfer leichter machen soll.

6.7.2 Physische Sicherheit

Bei der physischen Sicherheit geht es darum, physische Einwirkungen auf IT-Systeme abzuwehren oder gar nicht erst entstehen zu lassen. Dazu gehören Maßnahmen wie bspw. ein verschlossenes Rechnergehäuse oder ein geschützter Zugang zu einem

Rechenzentrum.[143] Ein Angriff bei einem Red Teaming besteht dann darin, in ein Gebäude mit IT-Systemen zu kommen. Zu Beginn eines Physical Assessments sollte die Infrastruktur eines Gebäudes und die dazugehörigen Prozesse durch eine Besichtigung betrachtet werden. Falls vorhanden, bieten sich öffentliche Veranstaltungen, wie ein Tag der offenen Tür oder der Besuch einer Kantine an.

Das Ausnutzen einer physischen Schwachstelle kann durch eine unverschlossene Tür, Tailgating (siehe Kapitel 6.7), das Kopieren von Zugangskarten (z. B. mit Proxmark3) oder durch das Knacken von Schlössern erreicht werden. Die Technik, Schlösser mit einem speziellen Werkzeug ohne einen passenden Schlüssel und ohne das Schloss zu beschädigen, zu öffnen, wird als Lockpicking bezeichnet (siehe Abbildung 46: Lockpicking-Werkzeug).

Abbildung 46: Lockpicking-Werkzeug[144]

Da es viele Schlösser gibt, die dieselben Schlüsseltypen verwenden, kann auch ein Schlüsselbund mit Standardschlüsseln helfen, ein Schloss zu öffnen. Bspw. bei Netzwerkschränken oder einem Schlüsselkasten werden häufig standardisierte Schlösser eingesetzt.

Das U.S. Department of Energy hat im Dezember 2016 ein Physical Security Systems Assessment Guide (PSS) veröffentlicht. PSS beschreibt eine detaillierte Methodik, mit der ein Physical Assessment geplant, durchgeführt und abgeschlossen werden kann.[145] Der Standard kann als Grundlage dienen.

6.7.3 Technische Sicherheit

Die eingesetzte Software ist immer abhängig von der vorgefundenen Infrastruktur und den eingesetzten Technologien. Von vielen Dienstleistern werden selbstentwickelte Skripte und

[143] Vgl. *Luber, S./Schmitz, P.*, Was ist physische IT-Sicherheit?, 2018.
[144] *Trinity, G.*, Lockpicking Set, 2017.
[145] *Office of Cyber and Security Assessment/Office of Enterprise Assessments/U.S. Department of Energy*, Physical Security Systems, 2016.

Anwendungen verwendet. Häufig fielen Frameworks, wie Metasploit und PowerShell Empire, die auch aus Penetrationstests bekannt sind. Der Blog PentestIT hat eine ganze Liste von möglichen Open Source und kommerziellen Tools zur Angriffssimulation veröffentlicht.[146] Eine häufig eingesetzte Software, die im Interview genannt wurde, war Cobalt Strike. Aus diesem Grund wird in diesem Kapitel die Software Cobalt Strike betrachtet.

Raphael Mudge hat 2010 die Software Armitage entwickelt. Armitage ist ein grafisches Cyber-Attack-Management-Tool für das Metasploit-Projekt, das Ziele visualisiert und Exploits empfiehlt. Armitage ist ein Open-Source-Netzwerk-Sicherheits-Tool, welches gemeinsame Sitzungen und Kommunikation durch eine einzige Metasploit-Instanz ermöglicht. Aus dieser Basis wurde Cobalt Strike im Jahre 2012 entwickelt. Die erste Version ist eine Erweiterung vom Metasploit Framework, um gezielte Angriffe durchführen zu können und die Verteidigung zu umgehen. In der zweiten Version, die 2014 veröffentlicht wurde, konnten Threat Emulationen (dt. Bedrohungssimulationen) durchgeführt werden, was ein Post-Exploitation ermöglicht. Seit 2015 und der Version 3 ist Cobalt Strike eine Plattform für Red Team Operations und Angriffssimulationen. Mit der Software können Taktiken und Techniken eines fortgeschrittenen Gegners in einem Netzwerk nachgeahmt werden.[147] Cobalt Strike ist eine Threat Emulation Software, mit der gezielte Angriffe auf moderne Infrastrukturen durchgeführt werden können. Folgende Features werden durch Cobalt Strike zur Verfügung gestellt:

Tabelle 26: Features Cobalt Strike[148]

Feature	Beschreibung
Reconnaissance (dt. Aufklärung)	Herausfinden von clientseitigen Anwendungen und deren Versionsinformationen
Attack Packages (dt. Angriffspakete)	Durchführung von Web-Drive-by-Angriffen und Erstellen von Trojanern Es kann bspw. ein Java Applet Angriff, Microsoft Office Trojaner und ein Windows Trojaner erstellt werden, zudem bietet die Software ein Webseiten-Klon-Tool.
Spear Phishing	Durch die Software können Phishing-E-Mails erstellt, versendet und verfolgt werden.
Collaboration (dt. Kollaboration)	Mit dem Teamserver können Daten ausgetauscht, in Echtzeit kommuniziert und Systeme gesteuert werden.
Post Exploitation	Durch die vorhandenen Payloads kann ein fortgeschrittener Angreifer modelliert, PowerShell-Skripte ausgeführt, Tasteneingaben protokolliert, Screenshots erstellt und Dateien heruntergeladen werden.

[146] Vgl. *PenTestIT*, List of Adversary Emulation Tools - PenTestIT, 2018.
[147] Vgl. *Strategic Cyber LLC*, Cobalt Strike.
[148] Vgl. *Strategic Cyber LLC*, Features - Cobalt Strike.

Feature	Beschreibung
Cover Communication (dt. verdeckte Kommunikation)	Die Netzwerkindikatoren sind durch Profile anpassbar. Zur Kommunikation aus dem Netzwerk kann HTTP, HTTPS und DNS verwendet werden.
Browser Pivoting (dt. Browser umlenken)	Durch Browser Pivoting können Zwei-Faktor-Authentifizierungen umgangen und auf authentifizierte Browser-Sitzungen zugegriffen werden.
Reporting and Logging (dt. Protokollierung und Berichterstattung)	Die Berichte enthalten eine Zeitleiste und eine Liste von Indikatoren, die vom Red Team verwendet wurden. Diese Berichte können erstellt werden, damit die Angriffe für das Blue Team nachvollziehbar sind und können als PDF und Word-Datei exportiert werden.

In einem Red Teaming könnte Cobalt Strike verwendet werden, um bspw. eine bestimmte Softwareversion zu erfahren. Für die gefundene Softwareversion könnte in einer dedizierten Testumgebung ein Angriff, wie ein Web-Drive-by-Angriff, entwickelt werden. Sobald der Angriff erfolgreich getestet wurde, könnte eine Spear-Phishing E-Mail aus dem Framework verschickt werden, um ein oder mehrere Mitarbeiter davon zu überzeugen, den Link in der E-Mail zu öffnen und so ein IT-System zu kompromittieren. Cobalt Strike dient bei einer erfolgreichen Infizierung als Server, über den das Zielsystem gesteuert und weitere Schritte wie eine seitliche Bewegung im Netzwerk oder Rechte-Erweiterungen durchgeführt werden können. Auch weitere Exploits von anderen Frameworks wie Metasploit können verwendet werden. Zudem können Profiles entwickelt werden, um bestimmte Angriffe zu simulieren. Ein Profil ist eine Textdatei mit Richtlinien für den Server. Hier können die Indikatoren für eine Transaktion definiert und eine Payload abgeändert werden. Dies ist eine Schlüsseltechnology für die Angriffssimulationen (engl. Adversary Simulation). Mit unterschiedlichen Profiles können verschiedene APTs nachgebildet werden. In einem Github-Repository werden Beispiel Profile zur Verfügung gestellt. Durch das Framework erfolgt ein zentrales Logging und Reporting. Auch ein Netzwerk von kompromittierten IT-Systemen kann verwaltet und betrieben werden.

6.7.4 Fazit

Technische Angriffe sind stark abhängig von der eingesetzten Infrastruktur. Ein Framework, das im Kapitel beschrieben ist, ist Cobalt Strike. Cobalt Strike bietet eine Vielzahl von Möglichkeiten zum Einsatz bei einem Red Teaming. Durch ein zentrales Logging und Reporting kann die Nachvollziehbarkeit von einem Projekt effizient gewährleistet werden. Auch eine initiale Infizierung von einer Infrastruktur durch die Social-Engineering Methode Spear-Phishing kann realisiert werden.

Beim Social Engineering gibt es eine Vielzahl von Methoden, die es ermöglichen, eine Person zu einer unzulässigen Handlung zu bringen. Eine physische Schwachstelle kann mit Tailgating, Lock-Picking, Standardschlüsseln, Kopieren von Schlüsselkarten oder durch

offenstehende Türen ausgenutzt werden. Weitere Informationen zum Physical Assessment kann der Physical Security Systems Assessment Guide liefern.

7 Fazit

Die grundlegende Fragestellung dieser Masterarbeitet war, welchen Nutzen ein Red Teaming für den Kunden hat bzw. wie sinnvoll es ist, einen Test durchzuführen. Aus der Ausarbeitung geht hervor, dass Red Teaming einen Nutzen für den Kunden hat und es aufgrund der Bedrohungslage sinnvoll ist, einen Test durchzuführen. Der Aufwand und die Kosten von Red Teaming im Vergleich zu einem Audit oder Penetrationstest sind zwar wesentlich höher, es kann aber dabei helfen Schwachstellen zu identifizieren, Sicherheitsmaßnahmen abzuleiten oder Sicherheitsprozesse zu optimieren.

Durch den Vergleich der Methodiken wurde beschrieben, was Red Teaming im Vergleich zum Penetrationstest und Audit kennzeichnet. In der Methodik zur Einordnung kann abgelesen werden, dass Penetrationstest, Audit und Red Teaming in unterschiedlichen Bereichen nützlich sind. Dabei wurde die Erkenntnis gewonnen, dass eine gewisse Abfolge der Methodiken empfehlenswert ist bzw. nachvollziehbar wäre. So könnte bspw. ein Audit dazu verwendet werden, alle benötigten Sicherheitsanforderungen eines Standards zu prüfen. Mit einem Penetrationstest können ein oder mehrere Systeme auf Schwachstellen überprüft werden. Wenn ein gewisser Reifegrad erreicht ist, ist Red Teaming eine Methodik, die die Erkennungs- und Reaktionsfähigkeit der Unternehmen auf einen Sicherheitsvorfall verbessern kann.

Audit und Penetrationstest sind in der Regel einem Red Teaming vorzuziehen, da die Methodiken mehr in die Breite gehen und dabei helfen einen höheren Stand der Informationssicherheit zu erreichen und das mit geringerem Aufwand und Kosten.

Die Organisation, die ein Red Teaming beauftragt, sollte bereits einen hohen Reifegrad erreicht haben. Ebenfalls ist zu beachten, dass durch ein Red Teaming ein (hohes) Risiko entsteht, das unter Umständen zu einem (hohen) Schaden führen kann. Daher sollte das Red Team und deren Vorgehensweise sorgfältig ausgewählt werden. Durch weitere aufgestellte Thesen wurde kritisch hinterfragt, was bei einem Red Teaming beachtet werden muss.

Im letzten Abschnitt wurde ein methodisch und juristisch vertretbarer Weg, ein Red Teaming in einem Unternehmen durchzuführen, beschrieben. Hierzu wurden der Prozess und mögliche technische Umsetzungen – aufgeteilt auf personelle, physische und technische Sicherheit – beschrieben. Hierbei ist zu beachten, dass es bei Red Teaming nicht den einen Weg gibt, sondern diese von den Anforderungen und den Voraussetzungen im Projekt abhängig sind.

7.1 Zukunftsaussichten

Aktuell gibt es noch kein TIBER-EU Framework für Deutschland und keine Vorgabe, dies im Finanzsektor umzusetzen. Nach Aussagen in den Interviews und der Berichterstattung über

TIBER-EU können Unternehmen im Finanzsektor davon ausgehen, dass sie in Zukunft voraussichtlich Red Teaming im Unternehmen durchführen müssen. Daher ist es für diese Unternehmen empfehlenswert, sich mit der Umsetzung des TIBER-EU auseinanderzusetzen. Dabei sollte bspw. betrachtet werden, ob ein internes Red Team und die Expertise aufgebaut oder dies bei einem Dienstleister beauftragt wird.

Aufgrund der hohen Bedrohungslage kann davon ausgegangen werden, dass Unternehmen weiter aufrüsten und es zu einer Steigerung des Reifegrades kommt. Auch der Aufbau von Blue Teams oder Mitarbeiter, die darauf spezialisiert sind Angriffe zu erkennen ist ein nachvollziehbarer Schritt, den in Zukunft voraussichtlich immer mehr Unternehmen gehen werden. Anschließend das Blue Team, z. B. durch ein Red Teaming zu prüfen, wird daher wahrscheinlich ebenfalls häufiger vorkommen. Vor allem bei Organisationen mit hohem oder sehr hohem Schutzbedarf, sowie für kritische Infrastrukturen wird es zukünftig sinnvoll sein solche Sicherheitstests durchzuführen, sobald ein hoher Reifegrad erreicht ist. Es ist auch denkbar, dass es langfristig zum Stand der Technik werden könnte.

Aufgrund der aktuellen Lage kann man davon ausgehen, dass das Angebot und die Nachfrage nach Red Teaming weiter ansteigt, auch wenn Red Teaming nur für bestimmte Unternehmen eine sinnvolle Ergänzung zum Audit und Penetrationstest ist.

8 Literaturverzeichnis

Abolhassan, Ferri (Security Einfach Machen): Security Einfach Machen: IT-Sicherheit als Sprungbrett für die Digitalisierung: Springer-Verlag

The Association of Banks in Singapore (Red Team: Adversarial Attack Simulation Exercises, 2018): Red Team: Adversarial Attack Simulation Exercises: Guideliens for the Financial Industry in Singapore, <https://abs.org.sg/docs/library/abs-red-team-adversarial-attack-simulation-exercises-guidelines-v1-06766a69f299c69658b7dff00006ed795.pdf> [Zugriff: 2019-07-01]

AV-Test GmbH (Malware): Malware, <https://www.av-test.org/de/statistiken/malware/> [Zugriff: 2019-07-01]

— (AV-TEST Sicherheitsreport 2017/2018: Die aktuelle Analyse zur IT-Bedrohungslage, 2018): AV-TEST Sicherheitsreport 2017/2018: Die aktuelle Analyse zur IT-Bedrohungslage, <https://www.av-test.org/de/news/av-test-sicherheitsreport-20172018-die-aktuelle-analyse-zur-it-bedrohungslage/> [Zugriff: 2019-07-01]

Bartsch, Michael/Frey, Stefanie (Cyberstrategien für Unternehmen und Behörden, 2017): Cyberstrategien für Unternehmen und Behörden: Maßnahmen zur Erhöhung der Cyberresilienz, Wiesbaden: Springer Vieweg, 2017

— (Cybersecurity Best Practices, 2018): Cybersecurity Best Practices: Lösungen zur Erhöhung der Cyberresilienz für Unternehmen und Behörden, 2018

Beermann, Johannes/Schönbohm, Arne (Hacken für die gute Sache – Cybersicherheit auf dem Prüfstand, 2018): Hacken für die gute Sache – Cybersicherheit auf dem Prüfstand: Gastbeitrag in der Zeitschrift für das gesamte Kreditwesen, <https://www.bundesbank.de/de/presse/gastbeitraege/hacken-fuer-die-gute-sache-cybersicherheit-auf-dem-pruefstand-755208> [Zugriff: 2019-07-01]

Bitkom e.V. (Spionage, Sabotage und Datendiebstahl - Wirtschaftsschutz in der Industrie): Spionage, Sabotage und Datendiebstahl - Wirtschaftsschutz in der Industrie: Studienbericht 2018, <https://www.bitkom.org/sites/default/files/file/import/181008-Bitkom-Studie-Wirtschaftsschutz-2018-NEU.pdf> [Zugriff: 2019-07-01]

Brabetz, Sebastian (Penetrationstest vs. Schwachstellenscan: Wann Sie die richtige Wahl treffen, 2016): Penetrationstest vs. Schwachstellenscan: Wann Sie die richtige Wahl treffen, <https://medium.com/mod-it-services/penetrationstest-vs-schwachstellenscan-wann-sie-die-richtige-wahl-treffen-d63554ed31ec> [Zugriff: 2019-07-01]

Bratović, Ivan (MITRE ATT&CK and the Unified Kill Chain, 2019): MITRE ATT&CK and the Unified Kill Chain, <https://sgros-students.blogspot.com/2019/01/mitre-att-and-unified-kill-chain.html> [Zugriff: 2019-07-01]

BSI (BSI - G 5 Gefährdungskatalog Vorsätzliche Handlungen - IT-Grundschutz-Kataloge - G 5.42 Social Engineering): BSI - G 5 Gefährdungskatalog Vorsätzliche Handlungen - IT-

Grundschutz-Kataloge - G 5.42 Social Engineering, <https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/g/g05/g05042.html> [Zugriff: 2019-07-01]

— (Glossar - IT-Grundschutz-Kataloge): Glossar - IT-Grundschutz-Kataloge, <https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html> [Zugriff: 2019-07-01]

— (IS-Penetrationstest und IS-Webcheck): IS-Penetrationstest und IS-Webcheck, <https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Dienstleistungen/ISPentest_ISWebcheck/ispentest_iswebcheck_node.html> [Zugriff: 2019-07-01]

— (IS-Webcheck): IS-Webcheck: Sicherheits-Check für Webauftritte durch das BSI, <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Pentest_Webcheck/Beschreibung_Webcheck.pdf;jsessionid=7B8260DA89638BF39CC4DB182522BF45.1_cid360?__blob=publicationFile&v=5> [Zugriff: 2019-07-01]

— (Studie Durchführungskonzept für Penetrationstests): Studie Durchführungskonzept für Penetrationstests, <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Penetrationstest/penetrationstest.pdf?__blob=publicationFile&v=3> [Zugriff: 2019-07-01]

— (Ein Praxis-Leitfaden für IS-Penetrationstests, 2016): Ein Praxis-Leitfaden für IS-Penetrationstests, <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Pentest_Webcheck/Leitfaden_Penetrationstest.pdf?__blob=publicationFile&v=10> [Zugriff: 2019-07-01]

— (Die Lage der IT-Sicherheit in Deutschland 2018, 2018): Die Lage der IT-Sicherheit in Deutschland 2018 2018, S. 100, <https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/bsi-lagebericht-2018.pdf?__blob=publicationFile&v=3>

— (IS-Penetrationstest, 2018): IS-Penetrationstest: Penetrationstest von IT-Systemen durch das BSI, <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Pentest_Webcheck/Beschreibung_Pentest.pdf;jsessionid=7B8260DA89638BF39CC4DB182522BF45.1_cid360?__blob=publicationFile&v=5> [Zugriff: 2019-07-01]

— (Cyber-Sicherheit, 2019): Cyber-Sicherheit, <https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/cyber-sicherheit_node.html> [Zugriff: 2019-07-01]

— (IT-Sicherheit in kleinen und mittleren Unternehmen (KMU), 2019): IT-Sicherheit in kleinen und mittleren Unternehmen (KMU), <https://www.bsi.bund.de/DE/Publikationen/Studien/KMU/Studie_IT-Sicherheit_KMU.html> [Zugriff: 2019-07-01]

BSI/ISACA (Leitfaden Cyber-Sicherheits-Check, 2014): Leitfaden Cyber-Sicherheits-Check: Ein Leitfaden zur Durchführung von Cyber-Sicherheits-Checks in Unternehmen und Behörden, <https://www.allianz-fuer-

cybersicherheit.de/ACS/DE/_/Publikationen/leitfaden.pdf?__blob=publicationFile&v=4 > [Zugriff: 2019-07-01]

BSides Stuttgart (BSides Stuttgart - Because Cyber has no Knautschzone): BSides Stuttgart - Because Cyber has no Knautschzone, <https://www.bsidesstuttgart.org/> [Zugriff: 2019-07-01]

(c't 2019, Heft 6): c't 2019, Heft 6

CREST (CBEST Intelligence-Led Testing): CBEST Intelligence-Led Testing, <https://www.crest-approved.org/wp-content/uploads/CBEST-Implementation-Guide-v2.0.pdf> [Zugriff: 2019-07-01]

— (An introduction to CBEST): An introduction to CBEST, <https://www.gdssecurity.com/images/anintroductiontocbest.pdf> [Zugriff: 2019-07-01]

— (A guide for running an effective Penetration Testing programme, 2017): A guide for running an effective Penetration Testing programme, <https://www.crest-approved.org/wp-content/uploads/CREST-Penetration-Testing-Guide.pdf> [Zugriff: 2019-07-01]

— (About CREST, 2019): About CREST, <https://crest-approved.org/about-crest/index.html> [Zugriff: 2019-07-01]

— (Assurance in Information Security, 2019): Assurance in Information Security, <https://www.crest-approved.org/> [Zugriff: 2019-07-01]

Cyber Startup Observatory (The MITRE ATT&CK for Enterprise and the Cyber Kill Chain): The MITRE ATT&CK for Enterprise and the Cyber Kill Chain, <https://cyberstartupobservatory.com/wp-content/uploads/2019/03/ATT&CK_for_Enterprise&Cyber_Kill_Chain_2.pdf> [Zugriff: 2019-07-01]

Datenschutz.org (Datenschutz in Deutschland & der Europäischen Union, 2019): Datenschutz in Deutschland & der Europäischen Union, <https://www.datenschutz.org/> [Zugriff: 2019-07-01]

Decker, Bart de/*Zúquete, André* (Hrsg.) (Communications and multimedia security, 2014): Communications and multimedia security: 15th IFIP TC 6/TC 11 international conference, CMS 2014, Aveiro, Portugal, September 25 - 26, 2014 ; proceedings, Bd. 8735, Heidelberg: Springer, 2014

Deloitte (Red Team): Red Team: Unser Konzept zur Steigerung organisatorischer Resilienz, <https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/Red%20Team%20-%20Verbesserung%20der%20Unternehmensresilienz.pdf> [Zugriff: 2019-07-01]

ECB (ECB publishes European framework for testing financial sector resilience to cyber attacks, 2018): ECB publishes European framework for testing financial sector resilience to cyber attacks, <https://www.ecb.europa.eu/press/pr/date/2018/html/ecb.pr180502.en.html> [Zugriff: 2019-07-01]

— (TIBER-EU Framework, 2018): TIBER-EU Framework: How to implement the European framework for Threat Intelligence-based Ethical Red Teaming, <https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf> [Zugriff: 2019-07-01]

Eckert, Claudia (IT-Sicherheit, 2018): IT-Sicherheit: Konzepte - Verfahren - Protokolle, 10. Auflage, Berlin/Boston: De Gruyter Oldenbourg, 2018

Engel, Giora (Deconstructing The Cyber Kill Chain, 2014): Deconstructing The Cyber Kill Chain, <https://www.darkreading.com/attacks-breaches/deconstructing-the-cyber-kill-chain/a/d-id/1317542.> [Zugriff: 2019-07-01]

ENISA (ENISA Threat Landscape Report 2018, 2019): ENISA Threat Landscape Report 2018: 15 Top Cyberthreats and Trends, <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018/at_download/fullReport> [Zugriff: 2019-07-01]

FireEye (Branchenspezifische Bedrohungsdaten): Branchenspezifische Bedrohungsdaten, <https://www.fireeye.de/current-threats/reports-by-industry.html> [Zugriff: 2019-07-01]

— (Der beste Schutz vor Spear-Phishing-Angriffen): Der beste Schutz vor Spear-Phishing-Angriffen, <https://www.fireeye.de/current-threats/best-defense-against-spear-phishing-attacks.html> [Zugriff: 2019-07-01]

— (M-Trends 2018): M-Trends 2018, <https://www.fireeye.de/content/dam/collateral/de/rpt-mtrends-2018.pdf> [Zugriff: 2019-07-01]

Hackner, Thomas (Red and Tiger Teaming: Erfahrungsbericht aus 8 Jahren Spionageüberprüfungen, 2018): Red and Tiger Teaming: Erfahrungsbericht aus 8 Jahren Spionageüberprüfungen, <https://2018.it-sa.tv/> [Zugriff: 2019-07-01]

Hayes, Kirk (Penetration Test vs. Red Team Assessment: The Age Old Debate of Pirates vs. Ninjas Continues, 2016): Penetration Test vs. Red Team Assessment: The Age Old Debate of Pirates vs. Ninjas Continues, <https://blog.rapid7.com/2016/06/23/penetration-testing-vs-red-teaming-the-age-old-debate-of-pirates-vs-ninja-continues/> [Zugriff: 2019-07-01]

Helisch, Michael/Pokoyski, Dietmar/Beyer, Marcus (Security Awareness, 2009): Security Awareness: Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung, Wiesbaden: Vieweg + Teubner, 2009

Hellmann, Roland (IT-Sicherheit, 2018): IT-Sicherheit: Eine Einführung, Berlin: Walter de Gruyter GmbH, 2018

Herzog, Pete (Open Source Security Testing Methodology Manual (OSSTMM)): Open Source Security Testing Methodology Manual (OSSTMM), <http://www.isecom.org/research/> [Zugriff: 2019-07-01]

Herzog, Sascha (Red Team Assessments: Durchführung professioneller Angriffssimulationen, 2018): Red Team Assessments: Durchführung professioneller Angriffssimulationen, <https://2018.it-sa.tv/> [Zugriff: 2019-07-01]

Hillebrand, Annette u. a. (Aktuelle Lage der IT-Sicherheit in KMU): Aktuelle Lage der IT-Sicherheit in KMU: Kurzfassung der Ergebnisse der Repräsentativbefragung,

<https://www.wik.org/fileadmin/Sonstige_Dateien/IT-Sicherheit_in_KMU/Aktuelle_Lage_der_IT-Sicherheit_in_KMU_-_WIK.pdf> [Zugriff: 2019-07-01]

Hoppe, Tobias (Prävention, Detektion und Reaktion gegen drei Ausprägungsformen automotiver Malware, 2014): Prävention, Detektion und Reaktion gegen drei Ausprägungsformen automotiver Malware: Eine methodische Analyse im Spektrum von Manipulationen und Schutzkonzepten, <https://d-nb.info/1066295336/34> [Zugriff: 2019-07-01]

intersoft consulting services AG (Cybersecurity – Red Team vs. Blue Team, 2019): Cybersecurity – Red Team vs. Blue Team (2019), <https://www.datenschutzbeauftragter-info.de/cybersecurity-red-team-vs-blue-team/> [Zugriff: 2019-07-01]

IX-REDAKTION (iX Kompakt (2019) IT-Sicherheit): iX Kompakt (2019) IT-Sicherheit, [S.l.]: HEISE MEDIEN

Kersten, Heinrich u. a. (IT-Sicherheitsmanagement nach der neuen ISO 27001, 2016): IT-Sicherheitsmanagement nach der neuen ISO 27001: ISMS, Risiken, Kennziffern, Controls, Wiesbaden: Springer Vieweg, 2016

Knight, Alissa (ATT&CK Model - Data Driven Investor - Medium, 2019): ATT&CK Model - Data Driven Investor - Medium (2019), <https://medium.com/datadriveninvestor/att-ck-model-c40a113aab4> [Zugriff: 2019-07-02]

Kohlenberg, Toby (Red teaming probably isn't for you, 2017): Red teaming probably isn't for you, <https://de.slideshare.net/TobyKohlenberg/red-teaming-probably-isnt-for-you-81283357> [Zugriff: 2019-07-01]

Laufenburger, Robin (Zehn beliebte Social-Engineering-Methoden im Überblick, 2019): Zehn beliebte Social-Engineering-Methoden im Überblick (2019), <https://it-service.network/blog/2019/03/29/social-engineering-methoden/> [Zugriff: 2019-07-01]

Lockheed Martin Corporation (The Cyber Kill Chain): The Cyber Kill Chain, <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html> [Zugriff: 2019-07-01]

— (Lockheed Martin. Your Mission is Ours., 2019): Lockheed Martin. Your Mission is Ours.: About Lockheed Martin, <https://www.lockheedmartin.com/en-us/who-we-are.html> [Zugriff: 2019-07-01]

Luber, Stefan/Schmitz, Peter (Was ist ein Exploit?, 2017): Was ist ein Exploit?: Definition Exploit (Ausnutzung von Schwachstellen), <https://www.security-insider.de/was-ist-ein-exploit-a-618629/> [Zugriff: 2019-07-01]

— (Was ist ein Threat Intelligence Service?, 2017): Was ist ein Threat Intelligence Service?: Definition, <https://www.security-insider.de/was-ist-ein-threat-intelligence-service-a-629188/> [Zugriff: 2019-07-01]

— (Was ist physische IT-Sicherheit?, 2018): Was ist physische IT-Sicherheit?, <https://www.security-insider.de/was-ist-physische-it-sicherheit-a-712152/> [Zugriff: 2019-07-01]

Malone, Sean T. (Using an expanded Cyber Kill Chain Model to increase attack resiliency, 2018): Using an expanded Cyber Kill Chain Model to increase attack resiliency, <https://www.blackhat.com/docs/us-16/materials/us-16-Malone-Using-An-Expanded-Cyber-Kill-Chain-Model-To-Increase-Attack-Resiliency.pdf> [Zugriff: 2019-07-01]

Microsoft (Microsoft Enterprise Cloud Red Teaming, 2014): Microsoft Enterprise Cloud Red Teaming (2014), <https://download.microsoft.com/download/C/1/9/C1990DBA-502F-4C2A-848D-392B93D9B9C3/Microsoft_Enterprise_Cloud_Red_Teaming.pdf> [Zugriff: 2019-07-01]

Miessler, Daniel (When to Use Vulnerability Assessments, Pentesting, Red Teams, and Bug Bounties, 2016): When to Use Vulnerability Assessments, Pentesting, Red Teams, and Bug Bounties (2016), <https://danielmiessler.com/blog/when-vulnerability-assessments-pentesting-red-team-bug-bounties/> [Zugriff: 2019-07-01]

Ministry of Defence (A Guide to Red Teaming, 2013): A Guide to Red Teaming (2013), <https://www.act.nato.int/images/stories/events/2011/cde/rr_ukdcdc.pdf> [Zugriff: 2019-07-01]

— (Red Teaming Guide, 2013): Red Teaming Guide: Second Edition, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/142533/20130301_red_teaming_ed2.pdf> [Zugriff: 2019-07-01]

MITRE (Adversary Emulation Plans): Adversary Emulation Plans, <https://attack.mitre.org/resources/adversary-emulation-plans/> [Zugriff: 2019-07-01]

— (MITRE ATT&CK™, 2019): MITRE ATT&CK™, <https://attack.mitre.org/> [Zugriff: 2019-07-01]

NIST (NIST Special Publication 800-53 (Rev. 4)): NIST Special Publication 800-53 (Rev. 4): Security Controls and Assessment Procedures for Federal Information Systems and Organizations, <https://nvd.nist.gov/800-53/Rev4/control/CA-8#> [Zugriff: 2019-07-01]

— (Red Team/Blue Team Approach): Red Team/Blue Team Approach, <https://csrc.nist.gov/Glossary/Term/Red-Team-Blue-Team-Approach> [Zugriff: 2019-07-01]

o. V. (Schadprogramm, 2019): Schadprogramm, <https://de.wikipedia.org/wiki/Schadprogramm> [Zugriff: 2019-07-01]

Office of Cyber and Security Assessment/Office of Enterprise Assessments/U.S. Department of Energy (Physical Security Systems, 2016): Physical Security Systems: Assessment Guide, <https://www.energy.gov/sites/prod/files/2017/02/f34/PhysicalSecuritySystemsAssessmentGuide_Dec2016.pdf> [Zugriff: 2019-07-01]

Ott, Kevin (Red Teaming: Fortgeschrittene Bedrohungsanalysen durch simulierte Angriffe, 2018): Red Teaming: Fortgeschrittene Bedrohungsanalysen durch simulierte Angriffe, <https://2018.it-sa.tv/> [Zugriff: 2019-07-01]

OWASP (OWASP Testing Guide v4 Table of Contents): OWASP Testing Guide v4 Table of Contents,

<https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents> [Zugriff: 2019-07-01]

Peake, Christopher (Red Teaming: The Art of Ethical Hacking, 2003): Red Teaming: The Art of Ethical Hacking, <https://www.sans.org/reading-room/whitepapers/auditing/paper/1272> [Zugriff: 2019-07-01]

PenTestIT (List of Adversary Emulation Tools - PenTestIT, 2018): List of Adversary Emulation Tools - PenTestIT (2018), <http://pentestit.com/adversary-emulation-tools-list/> [Zugriff: 2019-07-01]

Pohl, Hartmut (Taxonomie und Modellbildung in der Informationssicherheit, 2004): Taxonomie und Modellbildung in der Informationssicherheit (2004), <https://www.softscheck.com/pdf/Taxonomie_und_Modellbildung_in_der_Informationssicherheit.pdf> [Zugriff: 2019-07-01]

Pols, Paul (The Unified Kill Chain, 2017): The Unified Kill Chain: Designing a Unified Kill Chain for analyzing, comparing and defending against cyber attacks, <https://www.csacademy.nl/images/scripties/2018/Paul_Pols_-_The_Unified_Kill_Chain_1.pdf> [Zugriff: 2019-07-01]

Rabe, L. (Marktanteile der meistgenutzten Suchmaschinen weltweit bis Mai 2019, 2019): Marktanteile der meistgenutzten Suchmaschinen weltweit bis Mai 2019, <https://de.statista.com/statistik/daten/studie/225953/umfrage/die-weltweit-meistgenutzten-suchmaschinen/> [Zugriff: 2019-07-01]

RedTeam Security (Full Force Red Teaming): Full Force Red Teaming, <https://www.redteamsecure.com/red-teaming/> [Zugriff: 2019-07-01]

Relia, Sanjeev (Cyber warfare, 2015): Cyber warfare: Its implications on national security, New Delhi, India: Vij Books India Pvt Ltd, 2015

SANS (About): About, <https://www.sans.org/about/> [Zugriff: 2019-07-01]

Scarfone, K. A. u. a. (Technical guide to information security testing and assessment): Technical guide to information security testing and assessment, <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf> [Zugriff: 2019-07-01]

Schonschek, Oliver (Social Engineering – was Sie dazu wissen müssen, 2019): Social Engineering – was Sie dazu wissen müssen, <https://www.datenschutz-praxis.de/fachartikel/social-engineering-wie-nutzer-selbst-gehackt-werden/> [Zugriff: 2019-07-01]

Schonschek, Oliver/Schmitz, Peter (Cyber Kill Chain - Grundlagen, Anwendung und Entwicklung, 2017): Cyber Kill Chain - Grundlagen, Anwendung und Entwicklung: Was ist die Lockheed Martin Cyber Kill Chain?, <https://www.security-insider.de/cyber-kill-chain-grundlagen-anwendung-und-entwicklung-a-608017/> [Zugriff: 2019-07-01]

Searle, Elly (Helping Non-Security Stakeholders Understand ATT&CK in 10 Minutes or Less, 2019): Helping Non-Security Stakeholders Understand ATT&CK in 10 Minutes or Less (2019), <https://www.crowdstrike.com/blog/helping-non-security-stakeholders-understand-attck-in-10-minutes-or-less/> [Zugriff: 2019-07-01]

searx.me (About searx): About searx, <https://searx.me/about> [Zugriff: 2019-07-01]

Sikora, Axel (Security im Überblick (Teil 1): Einführung in die Kryptographie, 2003): Security im Überblick (Teil 1): Einführung in die Kryptographie: Safety und Security, <https://www.tecchannel.de/a/einfuehrung-in-die-kryptographie,402017,2> [Zugriff: 2019-07-01]

Sjouwerman, Stu (Democratic National Committee Thought it was Under Attack (It Was A Red Team Phishing Test…)): Democratic National Committee Thought it was Under Attack (It Was A Red Team Phishing Test…), <https://blog.knowbe4.com/democratic-national-committee-thought-it-was-under-attack-it-was-a-red-team-phishing-test> [Zugriff: 2019-07-01]

Small, Prescot (Defense in Depth: AnImpractical Strategy for a Cyber World, 2018): Defense in Depth: AnImpractical Strategy for a Cyber World, <https://www.sans.org/reading-room/whitepapers/warfare/paper/33896> [Zugriff: 2019-07-01]

Solmecke, Christian (Penetrationstest): Penetrationstest, <https://www.wbs-law.de/it-recht/computerkriminalitaet/penetrationstest/> [Zugriff: 2019-07-01]

Sowa, Aleksandra/Duscha, Peter/Schreiber, Sebastian (IT-Revision, IT-Audit und IT-Compliance, 2019): IT-Revision, IT-Audit und IT-Compliance: Neue Ansätze für die IT-Prüfung, 2. Aufl. 2019, 2019

Storm, Blake (ATT&CK™, 2018): ATT&CK™: ATT&CK 101, <https://medium.com/mitre-attack/att-ck-101-17074d3bc62> [Zugriff: 2019-07-01]

Storm, Blake E. u. a. (MITRE ATT&CK™: Design and Philosophy, 2018): MITRE ATT&CK™: Design and Philosophy, <https://www.mitre.org/sites/default/files/publications/pr-18-0944-11-mitre-attack-design-and-philosophy.pdf> [Zugriff: 2019-07-01]

Strategic Cyber LLC (Cobalt Strike): Cobalt Strike: Advanced Threat Tractics for Penetraion Testers, <https://www.cobaltstrike.com/> [Zugriff: 2019-07-01]

— (Features - Cobalt Strike): Features - Cobalt Strike, <https://www.cobaltstrike.com/features> [Zugriff: 2019-07-01]

Strobel, Steffan (Sprechen Sie Security?): Sprechen Sie Security?: Security-Fachchinesisch erklärt, c't 2019, Heft 6, S. 76–79

Thode, Jan (Arbeitgeber ist kein Diensteanbieter im Sinne des TKG wenn die private Internetnutzung erlaubt ist, 2016): Arbeitgeber ist kein Diensteanbieter im Sinne des TKG wenn die private Internetnutzung erlaubt ist, <https://www.datenschutz-notizen.de/arbeitgeber-ist-kein-diensteanbieter-im-sinne-des-tkg-wenn-die-private-internetnutzung-erlaubt-ist-3914254/> [Zugriff: 2019-07-01]

Thommen, Jean-Paul/Achleitner, Ann-Kristin/Gilbert, Dirk Ulrich (Allgemeine Betriebswirtschaftslehre, 2017): Allgemeine Betriebswirtschaftslehre: Umfassende Einführung aus managementorientierter Sicht, 8., vollständig überarbeitete Auflage, 2017

Trinity, Geo (Lockpicking Set, 2017): Lockpicking Set, <https://de.wikipedia.org/wiki/Lockpicking#/media/Datei:Lockpicking-Set.jpg> [Zugriff: 2019-07-01]

Wege, Oliver (Datei:Defense-in-Depth1.png, 2016): Datei:Defense-in-Depth1.png, <http://www.secupedia.info/w/index.php?title=Datei:Defense-in-Depth1.png&filetimestamp=20160919081937&> [Zugriff: 2019-07-01]

Weidele, Max (Warum Ihre nächste Security-Investition nach Defense-In-Depth erfolgen sollte, 2018): Warum Ihre nächste Security-Investition nach Defense-In-Depth erfolgen sollte, <https://www.sichere-industrie.de/warum-ihre-naechste-security-investition-nach-defense-in-depth-erfolgen-sollte/> [Zugriff: 2019-07-01]

Anlage 1 Interview Cyber-Security-Practitioner

Beruf: IT-Sicherheitsberater für ISMS mit 12 Jahre Berufserfahrung
Qualifikation: ISMS 27001 Auditor/ Cyber Security Practitioner

Wie ist deine persönliche Erfahrung mit CSC-Projekten?

- Jährlich werden ca. zwei CSC bei Unternehmen durchgeführt.
- Kunden sind hauptsächlich kleine und mittelständische Unternehmen, die nur wenige oder keine Dokumentationen bezüglich Informationssicherheit haben. Der CSC kann aber mit jeder Unternehmensgröße durchgeführt werden.
- Ergebnisse wurden sehr positiv von den Kunden aufgenommen, da es einen guten Überblick über aktuelle Sicherheitsmängel und Verbesserungspotenziale gibt.
- Die Unternehmen sind rein technisch gesehen, oft sehr gut aufgestellt, allerdings gibt keine oder wenig Dokumentationen (z. B. Richtlinien).
- Betrachtet man alle CSCs dann ist festzustellen, dass nur wenig Dokumentation vorhanden ist und es häufig Single Point of Failures gibt, d. h., dass beim Ausfall eines einzelnen Bestandteils es zum Ausfall eines gesamten Systems führen kann. So ist bspw. das Wissen über ein System nur bei einer Person vorhanden und keine Systemdokumentation vorhanden.

Was sind die großen Vor- und Nachteile des CSC?

- Die Unternehmen können ohne Dokumentation von Sicherheitsprozesse oder sich mit der ISMS, ISO 27001 oder IT-Grundschutz auseinander gesetzt zu haben auf den aktuellen Stand der Cyber-Sicherheit prüfen lassen.
- Es gibt einen Einblick darauf, wie gut die „Kronjuwelen“ des Unternehmens abgesichert sind.
- Der CSC kann bei jeder Unternehmensgröße durchgeführt werden und kann auch individuelle auf einen Kunden angepasst werden.
- Für die Durchführung eines Audits ist keine Schutzbedarfsanalyse notwendig.
- Der Ergebnisbericht listet die Mängel und Problematiken auf.
- Zu beachten ist, dass die Prüfung eine logische Sicherheitsprüfung ist, die hauptsächlich auf Grundlage von Interviews beruht. Das Ergebnis ist von der Ehrlichkeit und dem Wissen des Interviewten abhängig.
- Beim CSC geht es um digitale Angriffe. Die physische Sicherheit wird nicht geprüft.

Wie wird ein CSC durchgeführt?

Der CSC beginnt mit einem Angebot. Im Angebot werden folgenden Arbeitspakete für die Durchführung eines CSC beschrieben:

AP 1 Erstellen einer Cyber-Sicherheits-Exposition

Zur Risikoersteinschätzung für die Rettungsleitstelle wird vor der Vor-Ort-Beurteilung die Cyber-Sicherheits-Exposition bestimmt, respektive die vorhandene Risikoanalyse bewertet. Dabei steht der komplette Informationsverbund im Fokus. Darauf basierend kann der zu

erwartende Zeitaufwand, die Beurteilungstiefe sowie die Wahl der Stichproben risikoorientiert bestimmt werden. Detaillierte Informationen zur Bestimmung der Cyber-Sicherheits-Exposition finden sich in der BSI-Empfehlung zur Cyber-Sicherheit BSI-CS_013 „Cyber-Sicherheits-Exposition“. Dieses Arbeitspaket wird vor-Ort innerhalb von ca. 3 Stunden erarbeitet und dient als Grundlage für die weitere Bearbeitung.

AP 2 Dokumentensichtung

Die Dokumentensichtung dient dazu, einen Überblick über

- die Aufgaben,
- die Organisation und
- die IT-Infrastrukturen der Institution

zu gewinnen. Die Dokumentensichtung beinhaltet lediglich eine grobe Sichtung der zur Verfügung gestellten Dokumente. Hierbei werden (soweit vorliegend) insbesondere das IT-Rahmenkonzept, die Liste der kritischen Geschäftsprozesse, die Sicherheitsleitlinie und das Sicherheitskonzept inklusive Netzplans beurteilt.

AP 3 Vorbereitung der Vor-Ort-Beurteilung

Zur Vorbereitung der Vor-Ort-Beurteilung wird ein Ablaufplan unter Einbeziehung der Cyber-Sicherheits-Exposition erstellt. Dieser stellt dar, welche Inhalte wann beurteilt werden sollen und welche Ansprechpartner (Rollen/Funktionen) hierzu erforderlich sind. Der Ablaufplan wird vorab bereitgestellt.

AP 4 Vor-Ort-Beurteilung

Die Vor-Ort-Beurteilung selbst beginnt immer mit einem kurzen Eröffnungsgespräch und endet mit einem Abschlussgespräch. Im Eröffnungsgespräch wird der Institution die Vorgehensweise und Zielrichtung des Cyber-Sicherheits-Checks erläutert. Außerdem werden organisatorische Punkte geklärt, wie z. B. Zutrittskontrolle, Besprechungsraum oder etwaige Änderungen zum Ablauf. Die Beurteilung kann im Normalfall eine Woche nach Fertigstellung von AP1 durchgeführt werden.

AP 5 Erstellung des Mängelberichts

Der Cyber-Sicherheits-Check wird mit einem Beurteilungsbericht abgeschlossen. Der Bericht eröffnet einen Überblick zur Cyber-Sicherheit in der Institution und beinhaltet neben der Darlegung der Cyber-Sicherheits-Exposition eine Liste der festgestellten Mängel. Zu jedem Maßnahmenziel wird das jeweilige Beurteilungsergebnis dokumentiert. Dieser Mängelbericht wird Ihnen anschließend bereitgestellt.

AP 6 Durchführung eines Kurz-Audits

Die Durchführung des Kurz-Audits erfolgt an zwei aufeinanderfolgenden Tagen vor Ort. Für die Erstellung des Berichts wird angenommen, dass dafür nochmal 3 Tage im Back-Office benötigt werden. Da häufig keine Dokumente vorhanden sind entfällt der AP 2 Dokumentensichtung in den meisten Projekten.

Die Cyber-Sicherheits-Exposition kann sowohl telefonisch als auch Vor-Ort durchgeführt werden. Um sich persönlich kennen zu lernen, wird ein Vor-Ort Termin meistens von den Kunden bevorzugt.

Sobald der Auftrag erteilt wurde, geht der Cyber-Security Practitioner nach dem Leitfaden-Cyber-Sicherheits-Check der vom BSI und ISACA zur Verfügung gestellt wird vor

(https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/Publikationen/leitfaden.pdf?__blob=publicationFile&v=4).
Weitere Informationen können den folgenden Dokumenten entnommen werden:

- [ACS1] Allianz für Cyber-Sicherheit, Webauftritt, www.allianz-fuer-cybersicherheit.de
- [ACS2] Allianz für Cyber-Sicherheit, BSI-CS_013 „Cyber-Sicherheits-Exposition“, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_013.html
- [ACS3] Allianz für Cyber-Sicherheit, BSI-CS_006 „Basismaßnahmen der Cyber-Sicherheit“, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_006.pdf
- [ACS4] Allianz für Cyber-Sicherheit, Verbindliche Maßnahmenziele für den Cyber-Sicherheits-Check, Anhang vom Leitfaden
- [ACS5] Allianz für Cyber-Sicherheit, BSI-CS_072 „Erste-Hilfe bei einem APT-Angriff“, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_072_TLP-White.pdf?__blob=publicationFile&v=7
- [ACS6] Allianz für Cyber-Sicherheit, Muster-Bericht für den Cyber-Sicherheits-Check, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/Publikationen/muster.html?nn=6644004

Auf Grundlagen der Maßnahmenziele des Leitfadens wurde ein Fragenkatalog entwickelt der im CSC verwendet wird.
Der Plan für den Vor-Ort-Termin ist ähnlich einem ISMS Audit-Plan. Eine Agenda könnte folgendermaßen aussehen:

Workshop 1 Bestimmung der Cyber-Sicherheits-Exposition (Schutzbedarfsfeststellung)

1a Bedrohungsgrad

- Wert der Informationen und Prozesse
- Attraktivität für Angreifer
- Charakterisierung der Angreifer
- Zielgerichtetheit der Cyber-Angriffe
- Erfahrungswerte über Angriffe in der Vergangenheit

1b Transparenz

- Welche Informationen über den Aufbau der zu schützenden Infrastruktur sind öffentlich verfügbar?
- Können Angreifer mit technischen Methoden Einzelheiten der Infrastruktur aufklären?
- Werden über die Behörde oder das Unternehmen von Dritten in halboffenen oder geschlossenen Foren im Internet Informationen gesammelt, die für Angreifer, die diese Foren beobachten, von Nutzen sein könnten?
-

Workshop 2 Cyber-Sicherheitsniveau definieren

- Absicherung der Netzübergänge
  - Identifikation
  - Segmentierung
  - Sicherheitsgateways
  - Absicherung mobile Zugänge

- Abwehr von Schadprogrammen
- Inventarisierung
- Umgang Sicherheitslücken
    - Patchmanagement
    - Workarounds und Sicherheitsaktualisierungen
- Interaktion mit dem Internet
    - Browser
    - E-Mail
    - Dokumentendarstellung
- Logdatenerfassung und –auswertung
- Sicherstellung eines aktuellen Informationsstandes
- Bewältigung von Sicherheitsvorfällen
- Sichere Authentisierung
- Gewährleistung der Verfügbarkeit notwendiger Ressourcen
- Durchführung nutzerorientierter Maßnahmen
- Sichere Nutzung Sozialer Netzwerke
- Durchführung von Penetrationstests

Nachdem durchgeführten Workshops wird der Bericht mit den Mängeln erstellt. Beispiele aus einem Ergebnisbericht:

- Bewertung aus der Cyber-Sicherheits-Exposition inkl. Beschreibung.

Vertraulichkeit	Integrität	Verfügbarkeit
Hoch	Hoch	Normal

- Ausschnitt aus der Mängelliste / Status der Cyber-Sicherheit

Nr.	Maßnahmenziel	Bewertet	Ergebnis
A	Absicherung von Netzübergängen	Ja	Sicherheitsmängel festgestellt
B	Abwehr von Schadprogrammen	Ja	Sicherheitsmängel festgestellt
C	Inventarisierung der IT-Systeme	Ja	Keine Mängel festgestellt

- Detaillierte Bewertungsergebnisse inklusive Beschreibung des Sicherheitsmangel und Empfehlungen.

Maßnahmenziel	A – Absicherung von Netzübergängen
Ergebnis	Sicherheitsmängel festgestellt
Ansprechpartner	
Stichproben	Mail-Konzept, Firewall, WLAN

Sicherheitsmangel:

Es gibt derzeit keine klaren Regelungen zum Austausch von Daten mit Dritten. Dadurch werden schutzbedürftige Daten ggf. ungesichert übermittelt.

Empfehlung:

Der Einsatz einer selbst gehosteten bzw. unter der eigenen Kontrolle befindlichen cloudbasierten Lösung zum sicheren Austausch von Informationen mit Dritten wird empfohlen.

Gibt es sonstige Hinweise zum CSC?

- Der aktuelle Leitfaden für den CSC wird im Moment überarbeitet. Hierbei wird die Cyber-Sicherheits-Exposition (CSE) angepasst, da die bisherige CSE oft einen hohen Schutzbedarf ergab, der nach der Einschätzung des Unternehmens und dem Cyber-Security-Practitioner nicht nachvollziehbar war.
- Die Kunden melden sich häufig bei Dienstleister und wollen einen Penetrationstest durchführen mit dem Ziel den Stand der Informationssicherheit zu prüfen. Hier wird den Kunden empfohlen einen CSC durchzuführen, da dies einen Überblick über den Stand der Cyber-Sicherheit gibt und eine technische Überprüfung, wie ein Penetrationstest für die Unternehmen häufig nur eine geringe Aussagekraft hat.
- Wenn ein Kunde bereits ein ISMS nach ISO 27001 oder IT-Grundschutz umgesetzt hat oder die Umsetzung plant bzw. eine Zertifizierung anstrebt, dann ist es zu empfehlen einen ISMS bzw. IT-Grundschutz-Umsetzungsworkshop durchzuführen. Anhand einer GAP-Analyse wird dem Kunden dabei aufgezeigt, welche Schritte zur Umsetzung bis zur Zertifizierung notwendig sind. Wenn keine Zertifizierung angestrebt bietet sich ein CSC an.
- Aus dem CSC ergibt sich häufig, dass keine Penetrationstests durchgeführt wurden und es für manche Systeme zu empfehlen ist, diese technisch zu prüfen.
- Ziel des Dienstleisters ist es den Cyber-Sicherheits-Check stärker zu werben und die Anzahl der „*Cyber-Security Partitionier*“ zu erhöhen im Unternehmen zu erhöhen.

Anlage 2 Marktübersicht

Nr.	Firmenname	Kontinent	Hauptsitz	Land	Branche	Mitarbeiteranzahl	Größenkategorie	Gegründet	Spezialgebiete
1	Deloitte	Amerika	New York	USA	Management-Beratung	10.001+ Mitarbeiter	Groß	1845	Audit, Consulting, Financial Advisory, Risk Management und and Tax services
2	CIPHRON GmbH	Europa	Hannover	Deutschland	IT und Services	11 bis 50 Mitarbeiter	Klein	2009	IT-Security, Open Source Engineering und Software Development
3	NSIDE ATTACK LOGIC	Europa	München	Deutschland	Computer- & Netzwerksicherheit	11 bis 50 Mitarbeiter	Klein	2014	Penetration Tests, Red Teaming, IT Security Workshops/Trainings, Web App Hacking, IoT Hacking, SCADA Hacking, Hardware Hacking, Social Engineering, Source Code Audits, Live Hacking, ATM Hacking, Industry 4.0, Software Development, White Hat Hacking, Research und Consultancy
4	aramido GmbH	Europa	Karlsruhe	Deutschland	Computer- & Netzwerksicherheit	2 bis 10 Mitarbeiter	Klein	2015	Security by Design, Umsetzungsbegleitung, Schwachstellenscans, Penetrationstests und IT-Notfallmanagement
5	RedTeam Security	Amerika	Saint Paul	USA	Computer- & Netzwerksicherheit	11 bis 50 Mitarbeiter	Klein	2008	security, penetration test, vulnerability, red team, tiger team, social engineering, scada und physical security
6	softScheck GmbH	Europa	Sankt Augustin	Deutschland	Computer- & Netzwerksicherheit	11 bis 50 Mitarbeiter	Klein	1998	Threat Modeling, Penetration Testing, Dynamic Analysis - Fuzzing, Zero-Day-Vulnerabilities, Sicherheitslücken, Smart Grid und Security by Design
7	TÜV Informationstechnik GmbH	Europa	Essen	Deutschland	IT und Services	51 bis 200 Mitarbeiter	Mittel	1995	IT Security, Automotive Security, Industrial Security, Mobile Security, Cyber Security, Data Center Security, eIDAS, Data Privacy, Common Criteria, Critical Infrastructure, Evaluation, Audits, Certification, KRITIS und Penetration Testing
8	F-Secure	Europa	Helsinki	Finnland	Computer-Software	1.001 bis 5.000 Mitarbeiter	Groß	1988	Security as a Service through Service Providers, Cyber security, Vulnerability Management, Endpoint protection, Incident Response, EDR, MDR, Cloud Security Services, Threat Intelligence, Red Teaming, VPN und Internet Security
9	Kalweit ITS GmbH	Europa	Hamburg	Deutschland	Computer- & Netzwerksicherheit	2 bis 10 Mitarbeiter	Klein	2018	Security Consulting
10	PricewaterhouseCoopers	Amerika	New York	USA	Buchhaltung	5.001 bis 10.000 Mitarbeiter	Groß	1998	Assurance, Tax und Advisory
11	Airbus CyberSecurity	Europa	Elancourt	Frankreich	IT und Services	501 bis 1.000 Mitarbeiter	Mittel	2003	Cyber Security, Cyber Defence, SOC Services, Penetration Testing, Incident Response, ICS Security, Cyber Consulting, Advanced Persistent Threats und Threat Intelligence
12	secunet Security Networks AG	Europa	Essen	Deutschland	Computer- & Netzwerksicherheit	501 bis 1.000 Mitarbeiter	Mittel	1997	Network Security, Encryption Technology, Public Key Infrastructures, Biometrics / eID, Data Protection, IT Compliance, Automotive Security, Homeland Security, Border Control, SINA, e-Government, Cryptography, IT Consulting, 5G, Edge und Cloud Computing
13	HACKNER Security Intelligence GmbH	Europa	Wien	Österreich	Sicherheits- & Ermittlungsdienste	2 bis 10 Mitarbeiter	Klein	2010	Red Teaming, Tiger Teaming, Penetration Testing und Vulnerability Management
14	Networking4ALL	Europa	Ansterdam	Niederlande	Internet	11 bis 50 Mitarbeiter	Klein	2000	Online security, Website security, Website scanning, SSL, Software signing, E-mail signing, Malware scanning, Network security, Vulnerability Management und Code Signing
15	FireEye	Europa	Milpitas	USA	Computer- & Netzwerksicherheit	1.001 bis 5.000 Mitarbeiter	Groß	2004	next generation threat protection, #infosec, zero-day exploits/malware, targeted attacks, network security, incident response, adaptive defense, #DFIR, #cybersecurity und #EndpointSecurity
16	Core Security	Amerika	Irvine	USA	Computer- & Netzwerksicherheit	51 bis 200 Mitarbeiter	Mittel	1996	penetration testing, security intelligence, software solutions, vulnerability research, threat expertise und threat modeling
17	Wizable	Europa	San Jose	USA	IT und Services	2 bis 10 Mitarbeiter	Klein	2007	Security Audits und PenTests Cyber Threat Intelligence Cyber Security Incident Response Team Cyber Security Incident Detection Services IT-Sicherheit Managed Security Services Informationssicherheit Cloud-Sicherheit Zusätzliche Dienstleistungen
18	Tryption	Europa	Biel	Schweiz	Computer- & Netzwerksicherheit	2 bis 10 Mitarbeiter	Klein	2018	Security Audit Consulting Red Teaming Social Engineering
19	KPMG	Europa	Amstelveen	Niederlande	Buchhaltung	10.001+ Mitarbeiter	Groß	1987	Advisory, Tax und Audit
20	A&O IT Group	Europa	Bracknell	Großbritannien	IT und Services	201 bis 500 Mitarbeiter	Mittel	1963	IT Services, Networking, Unified Communications, IT Service Management, Dynamic Services, Network Optimisation, Workspace Productivity, Hardware Support & Maintenance, Service Desk, IMAC und Breakfix

Nr.	Firmenname	Kontinent	Hauptsitz	Land	Branche	Mitarbeiteranzahl	Größenkategorie	Gegründet	Spezialgebiete
21	Context Information Security	Europa	London	Großbritannien	Computer- & Netzwerksicherheit	201 bis 500 Mitarbeiter	Mittel	1998	information security, penetration testing, application security specialists, forensic investigation, infrastructure security testing, Advanced Persistant Threat, cyber security und TADS
22	Deftact	Asien	Singapur	Singapur	Sicherheits- & Ermittlungsdienste	2 bis 10 Mitarbeiter	Klein	2016	Personal Covert Services Security Training Security Consulting
23	Secarma	Europa	Manchester	Großbritannien	Computer- & Netzwerksicherheit	51 bis 200 Mitarbeiter	Mittel	2001	Penetration Testing, Vulnerability Testing, Digital forensics, RAID data recovery, Web Application Assessment, Red Teaming, Infrastructure Testing, Industrial Control Systems, Cybersecurity Training und IoT
24	Synopsys	Amerika	Mountain View	USA	Computer-Software	10.001+ Mitarbeiter	Groß	1986	EDA, Computer Software, Semiconductor IP, Software Quality und Software Security
25	Pyramid Cyber Security & Forensic Pvt. Ltd	Asien	New Delhi	Indien	Sicherheits- & Ermittlungsdienste	51 bis 200 Mitarbeiter	Mittel	2008	Cyber Forensic Solutions, Security Information & Event Management (SIEM), Cyber Forensic Investigation, Incident Response Services, Information Protection Solutions, Security Operation Center (SOC), Managed Security Services (MSS), VAPT (Vulnerability Assessment & Penetration Testing), Web & Mobile Application Security, Multi-factor Authentication Solution, ISO 27001 Readiness For Certification, Cyber Security Compliance for Banks, Cyber Security Compliance for Insurance Companies, Source Code Review, Incident Response und Risk Assessment
26	Secura	Europa	Amsterdam	Niederlande	IT und Services	51 bis 200 Mitarbeiter	Mittel	2000	Technical IT security audits, penetration testing, vulnerability analysis, security by design, awareness and secure programming training, risk management, security and risk management und digital security
27	AWARE7 GmbH	Europa	Gelsenkirchen	Deutschland	IT und Services	2 bis 10 Mitarbeiter	Klein	2019	Sensibilisierung, Penetrationstests, Awareness, IT-Security, Cybersecurity, Red Teaming und Phishing
28	enableIT, LLC	Amerika	New York	USA	Management-Beratung	2 bis 10 Mitarbeiter	Klein	2009	Ethical Hacking, Financial Risk and Regulations, Big Data, Analytics, IOS and Android Security, OWASP Top 10 Remediation, Identity and Access Management, Agile, Lean Six Sigma, BRD, FRD, UAT, UX, IA und JAVA and *.JS Frameworks, C#, Python, Scala, R.
29	ARSEC SECURITY CONSULTING	Asien	Israel	Israel	Computer- & Netzwerksicherheit	2 bis 10 Mitarbeiter	Klein	2011	Security Training Threat & Risk Assessment Design & Technology Executive Protection Red Team Security Audits Travel Security Consulting
30	Red Scan	Europa	London	Großbritannien	Computer- & Netzwerksicherheit	11 bis 50 Mitarbeiter	Klein	2002	SOC as-a-service, Managed Detection and Response, Penetration Testing, Red Team Operations, Vulnerability Assessments, Information Security Assessments und Cyber Incident Response
31	Outflank	Europa	Amsterdam	Niederlande	Computer- & Netzwerksicherheit	2 bis 10 Mitarbeiter	Klein	2016	Red Teaming - Digital Attack Simulation - Incident Detection and Response
32	QCC Global Ltd	Europa	London	Großbritannien	Sicherheits- & Ermittlungsdienste	11 bis 50 Mitarbeiter	Klein	1999	Technical Surveillance Counter Measures (TSCM), Counter Espionage, Counter Surveillance, Electronic Bug Detection, Physcial Security Reviews, Tiger Testing Services, Incident Response, Permanent Bug Detection Solutions, High Net Worth Individuals, Cyber Forensics, Digital Forensics und Bug Sweeping
33	CBI | Cyber Security Solutions	Amerika	Detroit	USA	IT und Services	51 bis 200 Mitarbeiter	Mittel	1991	CBI Security Manager, Digital Forensics, Identity Management, Incident Response, Managed Services, Data Loss Prevention, Pen Testing, Vulnerability Management, Managed SEP, Encryption, Advisory Services, Compliance & Governance und Social Engineering
34	Redspin	Amerika	Austin	USA	Computer- & Netzwerksicherheit	201 bis 500 Mitarbeiter	Mittel	2000	Penetration Testing, Security Risk Assessment, HIPAA Risk Assessment, Social Engineering, Vulnerability Assessments und Application Security
35	Red Tiger Security	Amerika	Housten	USA	Sicherheits- & Ermittlungsdienste	11 bis 50 Mitarbeiter	Klein	2008	Cyber Security Assessments, SCADA Security, Industrial Control Systems Security und SCADA Security Training
36	Sense of Security	Australien	Sydney	Australien	IT und Services	11 bis 50 Mitarbeiter	Klein	2002	Information Security - Governance, Risk and Compliance, Penetration Testing, Cyber Security Strategy and Roadmap, Application Security, Payment Card Industry (PCI) - Data Security Standard, Threat and Vulnerability Management, Web Application Testing und ISO 27001 2013 Certified
37	Network Intelligence	Amerika	New York	USA	Computer- & Netzwerksicherheit	501 bis 1.000 Mitarbeiter	Mittel	2001	Information Rights Management, Penetration Testing, Vulnerability Assessment, Web application security, DLP, PCI DSS, ISO 27001, SCADA Assessment, Risk Assessment, Breach Response, Compliance, CoBIT, PA DSS, Sharepoint Security, DDos, MDM, 2FA, WAF und DAM
38	NTT Security	Europa	Isamaning	Deutschland	Computer- & Netzwerksicherheit	1.001 bis 5.000 Mitarbeiter	Groß	1988	Managed Security Services, Computer Security, SaaS, Cloud Security, PCI DSS, ISO 27001, Security Strategy, Penetration Testing, Application Security, Database Security, Network Security und Security Consulting

Nr.	Firmenname	Kontinent	Hauptsitz	Land	Branche	Mitarbeiteranzahl	Größenkategorie	Gegründet	Spezialgebiete
39	FortConsult | Part of NCC Group	Europa	Kopenhagen	Dänemark	Computer- & Netzwerksicherheit	51 bis 200 Mitarbeiter	Mittel	2002	IT Security, PCI, P2PE, Security Assessments, Mobile Security, Incident Response, Forensics, IT Security Consulting, Advanced Penetration Testing, IoT Security, Maritime Security und Managed Security Services
40	Sec-Research GmbH	Europa	Wien	Österreich	IT und Services	2 bis 10 Mitarbeiter	Klein	2015	IT-Security, ISO 27001, Information Security, Vulnerability Management, Identity Management, Security Awareness, Pentesting, ISMS und Cryptography
41	Fidus Information Security	Europa	Cambrige	Großbritannien	Computer- & Netzwerksicherheit	2 bis 10 Mitarbeiter	Klein	2017	Penetration Testing, Security Consultancy, ITHC, Infrastructure Testing, Red Teaming und Application Assessments
42	FortyNorth Security	Amerika	Castle Rock	USA	IT und Services	2 bis 10 Mitarbeiter	Klein	2018	Red Teaming, Penetration Testing, Web Application Assessments, Social Engineering, Wireless Network Assessments, Internal Penetration Test, External Penetration Test, Collaborative Red Teaming, Offensive Security, Cybersecurity Consulting, Vulnerability Assessment, Red Team Training und Cyber Security
43	Oxford Integrated Systems	Europa	Oxford	Großbritannien	IT und Services	2 bis 10 Mitarbeiter	Klein	2003	Cyber Security, Cyber Training, Cyber Consultancy und Cyber Accreditation
44	Syss GmbH	Europa	Tübingen	Deutschland	Computer- & Netzwerksicherheit	51 bis 200 Mitarbeiter	Mittel	1998	Penetrationstest Digitale Forensik Live-Hacking Schulung
45	Exploit Labs UG	Europa	Eschborn	Deutschland	Computer- & Netzwerksicherheit	2 bis 10 Mitarbeiter	Klein	2017	Penetration Testing Red Teaming Training
46	cirosec	Europa	Heilbronn	Deutschland	Computer- & Netzwerksicherheit	51 bis 200 Mitarbeiter	Mittel	2002	innovative security, implementation, consulting, trainings, pentesting, incident handling and forensic, information security and risk management und audits
47	Code White	Europa	Ulm	Deutschland	Computer- & Netzwerksicherheit	11 bis 50 Mitarbeiter	Klein	2014	IT Security, Intelligence Driven Security, Penetration Testing, Security Research und Redteam

Anlage 3 Interviewprotokoll Dienstleister

1. Beschreibung -Was ist Red Teaming bzw. ein Red Team Assessment?

Allgemeines

- Es ist das Testen von einem System (Unternehmen, Organisation, IT-System, Prozesse …) mit bestimmten Angriffen.
- Die (Geschäfts-) Prozesse werden gezielt angegriffen.
- Das Ziel ist es, einen Weg zum vorgegebenen Ziel zu finden. Dies kann durch Verkettung von unterschiedlichen Techniken erreicht werden.
- Im vorgelagerten Workshop mit dem Kunden werden die Bedrohungen, Ziele und „Kronjuwelen“ des Unternehmens sowie Zwischenziele (Flags), die erreicht werden sollen festgelegt.
- Es wird in einem Team mit einem spezifizierten Ziel möglichst realistisch, wie ein rechter Angreifer, erreicht werden. Die unterschiedlichen Personen im Team haben unterschiedliche Expertisen in verschiedenen Bereichen.
- Die Aufträge wurden zum Teil vom Incident Response oder Forensik Team auf Grund eines bereits vorgefallenen Sicherheitsvorfall initiiert.
- Im Test werden Angriffe nachgestellt, um zu prüfen, ob ein Angriff erneut erfolgreich wäre.
- Red Teaming ist eine IT-Sicherheitsdienstleistung, um zu überprüfen, wie gut die hausinterne Abwehr/ Verteidigung funktioniert.
- Die Angriffe wurden teilweise mit Forensiker abgestimmt, um die Zeitabläufe und die Vorgehensweise eines realen Angriffs nachzubilden. Hierzu wurden ähnliches System und Software nachgebildet.
- Beim Red Teaming wird ein Rahmen festgelegt was beim Test erlaubt ist und was nicht.
- Red Teaming ist von der Zeit und Expertise der Tester abhängig.
- Red Teaming sollte durchgeführt werden, wenn ein Vulnerability Assessment, Penetrationstests und es bestimmte Sicherheitsmaßnahmen bzw. Detektionsmechanismen eingesetzt werden und dies geprüft werden sollen.
- Die Testweise verfolgt einen ganzheitlichen Ansatz. Es werden zusätzlich zur Technik noch Menschen, Prozesse und die Kommunikation in einer Notfallsituation geprüft.
- Es ist eine praktische Überprüfung der Sicherheitstechnik, des Sicherheitsstand und kann sowohl organisatorisch als auch physikalisch Prüfungen beinhalten mit dem Ziel ein festgelegtes Ziel zu erreichen
- Viele Kundenanfragen wird ein Penetrationstest benötigt, aber ein Red Teaming angefragt.

- Damit keine Systeme angegriffen wird, dass nicht zum Kunden gehört, wird vor einem Angriff im täglichen Meeting nachgefragt, ob das System angegriffen wird und bspw. nicht Business kritisch ist.
- Der Begriff Red Teaming wird vom Zweck missbraucht, um eine ganzheitliche Prüfung und für zusätzliche Sensibilisierungsmaßnahmen durchzuführen.
- Es ist eher ein regelmäßiger Prozess anstatt eines Projekts, das abgeschlossen wird. Es ist schwierig intern ein großes Projekt aufzustellen. Es ist kein interner Kooperationswille von unterschiedlichen Personen da. Dies soll aber in Zukunft geschehen.
- Es gibt sowohl Unternehmen die Red Teaming bei einem Dienstleister beauftragen als auch welche die ein Dienstleister als Red Team beauftragen.
- Es gibt einen Unterschied zwischen einem „normalen“ Red Teaming und einem Threat Emulation, bei der eine bestimmte APT-Gruppe oder ein Angreifer-Profil getestet wird. Dies ist eine sehr Fortgeschrittene Testweise. Threat-based Red Teaming ist nochmal eine Stufe, Skill-Level höher.

Bedrohungsanalyse vs. keine Bedrohungsanalyse

- Es wird die aktuelle Bedrohungslage des Auftraggebers betrachtet. Als Grundlage für die Tests werden realistische Threat Models (Bedrohungsmodelle) definiert. Ein Beispiel dient ein anonyme Angriffsgruppe oder ein Innentäter mit bestimmtem Vorwissen, um ein Unternehmen zu kompromittieren.
- In Abstimmung mit dem Kunden werden Angriffsszenarien erarbeitet.
- Die größten Bedrohungen werden in Abstimmung mit dem Kunden (Threat Analysis) identifiziert.
- Ein Angriff soll möglichst realistische und ähnlich zu bekannten APT-Gruppen sein, was die TTPs, Tool-Chain und die Ziele angeht.
- Die Threat Models werden auf Grundlage von eigener Erfahrung und Berichten über APTs, Antivieren-Hersteller, Blog Posts, Hackergruppen, Incident Reports, Security Reports oder Governance Reports festgelegt. Auf Grundlage von den Threat Models werden Szenarien definiert.
- Beim Red Teaming sollen Angriffsszenarien durchgeführt werden, die in der Realität vorkommen und ein Proof-of-Concept (PoC) erstellt. Dem Unternehmen geht es nicht darum, an bestimmte sensible Daten zu kommen, sondern es reichen offensichtliche Beweise.
- Die ausgewählten Angriffsszenarios werden legitimiert. Es werden Mutmaßungen getroffen, um herauszufinden, wie wahrscheinlich ein Szenario ist. Beim Einsatz von Verschlüsselung, wird bspw. die Konfiguration geprüft.
- In dem Unternehmen werden einzelne Phasen von APT-Gruppen nachgestellt und geprüft, wie Schwachstellen ausgenutzt werden kann.

Standard vs. kein Standard

- Es wird sich an TIBER-EU Framework orienteiert, das MITRE ATT&CK-Framework verwendet und Rahmenwerke von CREST (z. B. CREST Simulated Target Attack and Response (STAR) hinzugezogen.
- Bei großen Unternehmen (z. B. einer Bank) werden die relevanten APTs ausgewählt. Hierzu wird die MITRE ATT&CK Matrix verwendet.
- Das TIBER-EU ist aktuell noch keine Vorgabe, sondern nur eine Empfehlung, allerdings geht man davon aus, dass es in Zukunft eine Vorgabe wird. Daher richten sich Banken bereits heute nach diesem Framework, da es voraussichtlich früher oder später Red Teaming durchführen muss.
- Bei bekannten APTs wird das ATT&CK-Framework als Nachschlagewerk genutzt. Zum Teil wird dies aus dem Bau auf Grundlage der eigenen Erfahrung entschieden. Das Framework wird hauptsächlich dazu genutzt eine einheitliche Sprache zu haben.
- Bei weiteren Tests werden unterschiedliche Quellen, wie bei Webanwendungen, OWASP.
- Bei der Vorgehensweise kann man sich an die Cyber Kill Chain von Lockheed Martin richten.
- Eine Leitlinie namens *„Red Team: Adversarial Attack Simulation Exercises – Guidelines for the Financial Industriy In Singapore“* wurde von der Bank of Singapore veröffentlicht und ist ein gutes Nachschlagewerk.
- Je nach Prüfungen werden Inhalte aus den BSI-Katalogen oder der OWASP betrachtet.
- Es wird kein Standard verwendet.
- Es gibt keinen praktikablen Standard.

Blue Team vs. kein Blue Team

- Es werden auch Tests bei Unternehmen ohne SOC / Blue Team durchgeführt.
- Das Blue Team ist in den Unternehmen sehr unterschiedlich ausgeprägt. Ein vernünftiges Team ist häufig das Security Operations Center (SOC) oder das Security Defense Center (CDC). Hierbei werden unterschiedliche Erkennungstechniken verwendet.
- Ein Network Operation Center (NOC) und Security Operation Center (SOC) ist häufig in der Rolle des Blue Teams. Auch andere Teams aus den Security-Audits, Logs-Analyse, DDoS-Testing und SIEM-Teams können dazu gezählt werden.
- Es gab auch Tests, bei dem es kein wirkliches Blue Team gab, sondern nur einzelne Mitarbeiter die sich um Administration von Netzwerk, Firewall, Cloud, DevOps, DevSec-Ops kümmern. Eine oder zwei Ansprechpartner für Security sind normalerweise in den Projekten vorhanden gewesen.
- Es gibt Kunden die in Blue Team (SoC) hatten und welche bei dem die Aufgabe zum Beispiel Logs zu prüfen auf mehrere IT-Mitarbeiter aufgeteilt wurde.
- Die Erkennung erfolgt über Anomalien in den Log-Auswertungen.
- Die Projekte wurden bei Unternehmen mit einem Blue Team aus mehreren Mitarbeitern bis zu Unternehmen mit geringer Sicherheit durchgeführt.

- In einem Blue Team werden SOC-Mitarbeiter / Incident Response, Log-Analysten und Threat Intelligence benötigt. Typisch ist auch ein Security Guart der ein Monitoring / Log auswertet. Das Incident Response Team hat die Aufgabe False Positivies auszuwerten und zu reduzieren. Die Threat Intelligence muss nach neuen Techniken forschen. Es gibt Unternehmen, bei denen das Blue Team nicht vorhanden ist, bis zu sehr gut ausgeprägt.
- Ein wichtiger Punkt ist, dass wenn kein Blue Teaming vorhanden ist, ist der Mehrwert von Red Teaming nicht vorhanden.
- Das Blue Team ist jeder der nicht im Red Team ist. Vor allem sind die Personen gemeint, die operative in der Verteidigung arbeiten, wie das SOC, CERT und Mitarbeiter. Generell ist aber jeder der ein Angriff erkennen kann im Blue Team.

Szenario basierter Test vs. Red Teaming / Blue Team Test

- Bei einem Szenario basierten Test ist kein SOC erforderlich.
- Ein Red Teaming macht nur dann Sinn, wenn es ein Blue Team gibt. Die alternative ist ein Szenario basierter Test.
- Bei kleineren Unternehmen wird beim Red Teaming darauf geachtet, was von außen erreichbar ist (z. B. Services, Wifi). Hierbei geht es häufig darum, ein Blue Team bzw. die Security auszubauen und zu lernen, wie man mit einem Sicherheitsvorfall umgeht.

Red Teaming vs. Purple Teaming

- Eine Ausprägung von Red Teaming ist das Purple Teaming bei dem eng mit dem Blue Team zusammengearbeitet wird, um Angriffe von einem Red Team zu erkennen.
- Es wird von Red, Blue und Purple Teams gesprochen, die verschiedene Aufgabengebiete haben.
- Manche kommen mit dem Ziel das eigene Blue Team zu testen. Nach Aussagen des Unternehmens sehen Sie zur Verbesserung des Blue Teams ein Test mit klarem Drehbuch und gezielten Tests und direkter Unterstützung beim Finden von Schwachstellen als eine bessere Möglichkeit das Blue Team zu verbessern. Um das Blue Team zu verbessern kann es auch sinnvoll sein einen Beobachter ins Blue Team zu setzen, der das Team bei den Angriffen unterstützt.

Informiert vs. uninformiert

- Nur das Management, Vorstand und IT-Sicherheitsbeauftragte wird über einen Test informiert. Es ist ein nicht angekündigter Test.
- Das Blue Team darf nicht informiert sein. Dies würde das Ergebnis verfälschen und der Realismusgrad wesentlich geringer wäre.

Black-Box vs. Grey-Box / White-Box

- Beim Red Teaming ist ein Blackbox-Test, bei dem keine genaue IP-Adresse festgelegt wird.

- Es wird das Grey Box Vorgehen empfohlen. Informationen z. B. über Zeichnungsberechtigte, Unternehmensstruktur und Kontrollinstanzen werden im Vorfeld ausgetauscht.

Technische Sicherheit vs. physische Sicherheit vs. Social Engineering

- Beim Red Teaming wird ein Unternehmen als Ganzes geprüft, d. h. alle eingesetzten Maßnahmen, sowie technische, menschliche und physische Prüfungen. In Abstimmung mit dem Kunden wird besprochen, welcher Themenbereich, wie stark geprüft wird.
- Ein Projekt kann mit oder ohne Social Engineering durchgeführt werden. Es kann auch ein rein technisches Red Teaming durchgeführt beidem nur auf technischen Weg versucht wird ins Unternehmen zu kommen.

Voller Scope vs. eingeschränkter Scope

- Das Red Team versucht ein offensichtliches und schwaches Glied in der Sicherheitskette ausfindig zu machen.
- Beim Angriff gibt es wenig oder keine Einschränkungen.
- Es sollte, wie bei einem realen Angriff, ein möglichst kompletter Scope vorliegen.
- Da ein Full-Scope Red Teaming zu aufwändig und teuer wäre werden häufig einzelne Pakete geschnürt. Ein voller Scope und „richtiges Red Teaming“ wird nur sehr selten beauftragt. Ein Paket kann z. B. Social Engineering, eine technische Prüfung oder eine physikalische Analyse sein. Die Zerlegung in Paket macht es für den Kunden besser nachvollziehbar. Es wird auch bspw. simuliert, dass ein Angreifer bereits im Unternehmen ist und als Innentäter agiert. Dadurch wird ein Red Teaming unrealistischer, aber effizienter und von der Aussagekraft gleich oder tlw. sogar höher. Der Test kann in mehrere Stufen eingeteilt werden, um es effizienter zu machen.
- Ein großes Projekt ist im Unternehmen schwierig durchzusetzen, dadurch werden nur einzelnen Phasen nachgestellt. Dabei werden relevante Angriffe ausgewählt und die Auswirkung geprüft. Es geht darum die Auswirkung klar zu machen.
- Der Betriebsrat und der Datenschutz müssen beachtet werden. Aus diesen Gründen kann sich eine Einschränkung im Scope geben.
- Die Angriffswege sind abhängig vom Scope. Es gibt sowohl Full Scope als auch eingeschränkte Tests. Dies werden mit dem Kunden festgelegt. Zudem werden die Angriffswege nach dem Information Gathering und der zur Verfügung stehen Zeit ausgewählt. Hier werden auch auf Erfahrungswerte zurückgegriffen und nach Wegen vorgegangen die häufig funktioniert haben. Dies können sowohl Schwachstellen in Webanwendungen, Webseiten, Phishing als auch physische Angriffe sein.
- Wenn der Kunde im Scope eine freie Wahl der Angriffe lässt, wird auch ein Physical Assessment gemacht. Es gibt aber auch Einschränkung auf technische und Phishing Angriffe.
- Es gibt zwar einen freien Scope, dieser soll aber kontrolliert und in Abstimmung mit dem White-Team geprüft werden.

- Es kann eine Einschränkung auf IP-Adresse, Webanwendung oder Dienst geben.

Realismus vs. Inszeniert

- Je nach Zeitbegrenzung im Red Teaming kann es sehr unrealistisch werden.
- Beim Testen wird je nach Threat Model von einer unterschiedlichen Position und mit unterschiedlichem Wissen gestartet (z. B. von innen oder von außen).
- Beim Red Teaming soll auch verdeutlicht werden, dass ein initial Kompromittierung immer passieren kann und es nur abhängig von der Zeit und Expertise der Angreifer ist.
- Der Kunde muss für sich entscheiden, ob so etwas benötigt wird. Er kommt häufig mit der Anfrage einen möglichst realistischen Test zu bekommen. Dieser wird dazu verwendet die Geschäftsführung zu überzeugen.
- Beim Auftrag kann es auch sein, das bestimmte Sicherheitsmaßnahmen überwunden werden.

Frei Wahl der Angriffe vs. festgelegtes Angriffe

- Es bietet Freiraum bei der Auswahl der Angriffe, TTP, Tools und Methoden für den Tester. Es gibt keine vorgegebene Vorgehensweise und Drehbuch.
- Es werden unterschiedliche Angriffsmethoden ausgewählt.
- Beim Red Teaming werden gewissen Grenzen gesetzt bzw. die Freiheiten festgelegt.

Viele Angriffswege vs. ein Angriffsweg

- Es ist ein Simulationsangriff aus Sicht eines realen Angreifers, der versucht auf dem Weg des geringsten Widerstands in ein Unternehmen einzudringen.

Empfehlung

- Red Teaming sollte man erst dann durchführen, wenn man der Meinung ist, dass bereits ein gutes Sicherheitskonzept vorhanden ist. Es ist die ultimative Probe des Sicherheitskonzepts.
- Unternehmen die eine gewissen Reifegrad wie ein bestehendes SOC oder viele Penetrationstest durchgeführt haben, kann ein Red Teaming empfehlenswert sein.

2. Ziel - Was ist das Ziel von einem Red Teaming? Welche Ziele werden bei einem Red Teaming festgelegt?

Was ist das Ziel von Red Teaming?

- In einem Dokument der NATO („Cyber Red Teaming“) wird beschrieben, dass es bei Red Teaming darum geht die Erkennung von Angriffen bzw. das Blue Team zu verbessern.
- Das Hauptziel ist es einen Mehrwert für das Blue Team zu bekommen. Das Red Team muss sich immer hinterfragen, wie kann dem Blue Team geholfen werden?
- Es stellt eine gezielte Übung dar, wie gut die Verteidigung / Abwehr funktioniert.
- Ziel ist zu prüfen, wie gut das Blue Team oder die Sicherheitsmaßnahmen funktionieren.

- Das Ziel ist es das Blue Team zu unterstützen Angriffe zu erkennen.
- Mit Red Teaming soll das Computer Emergency Response Team (CERT) in der Regel getestet und involviert werden.
- Bei einem Red Teaming wird die Sicherheitsabteilung (Blue Team) einbezogen und getestet.
- Beim Red Teaming steht das Training des Blue Team (Security Operation Center (SOC)) im Vordergrund.
- Es sollen die Erkennungsmöglichkeiten im Unternehmen ausgetestet werden.
- Das Ziel von Red Teaming ist es, die Erkennung- und Reaktionsfähigkeit zu testen und zu messen.
- Das Red Team versucht, wenn es im Netzwerk ist eine Verbindung nach außen aufzubauen ohne das es vom Blue Team erkannt wird. Hierbei ist eine wichtige Kenngröße der Zeitpunkt wann ein Angriff detektiert/ erkannt wird. Der Angriffs- und Erkennungszeitpunkt wird daher sorgfältig dokumentiert.
- Es soll herausgefunden werden, ab wann ein Angriff erkannt wird und wie gut ein Unternehmen hinsichtlich Security aufgestellt ist.
- Das Red Team ist ein Service für das Blue Team, das versucht typische Angriffsarten zu erkennen.
- Ziel war es, das die eingesetzten Sicherheitsmechanismen und Maßnahmen geprüft werden, ob diese ausreichend sind ein simulierten/ nachgestellten Angriff abzuwehren.
- Hauptziel ist herauszufinden, welche Maßnahmen notwendig sind, um die Sicherheit im Unternehmen weiterzuentwickeln.
- Ein Teilziel ist auch Krisendokumentationen zu erstellen und zu dokumentieren, wie mit einem Angriff umgegangen werden soll.
- Die Security-Awareness soll verbessern werden, z. B. bei einem Phishing-Angriff.
- Ziel ist es, Wege aufzuzeigen und dem Kunden zu präsentieren.
- Mit Red Teaming wird versucht auf effizienten Weg an die „Kronjuwelen“ zu kommen.
- Red Teaming wird eingesetzt um das Blue Team (in der Regel ein SOC) länderübergreifend zu prüfen.
- Beim Red Teaming werden Flags im Netzwerk festgelegt die erreicht werden sollen (Beispiel sind bestimmte Dokumente oder ein privilegierter Benutzer).
- Banken haben häufig bereits ein Threat Intelligence Feed, der die relevanten Bedrohungen bzw. APTs kennt.
- Zudem können öffentlich verfügbare Thread Intelligence von TI-Provider verwendet werden, z. B. vom MITRE ATT&CK Framework oder FireEye verwendet werden.
- Bei der Prüfung der Kommunikation wird bspw. betrachtet, welche Schulungen bezüglich Security-Awareness und Phishing durchgeführt wurden. Es soll herausgefunden werden, ob die Maßnahmen ausreichend sind und sich die Sicherheitskosten amortisieren.
- Unternehmen wollen durch ein Red Teaming auch herausfinden, ob ein SoC wirklich benötigt wird.

- Unternehmen führen Red Teaming durch, da Sie zum Teil Angst vor bestimmten Angreifern haben, die bestimmte Daten veröffentlichen.

Welche Ziele wurden im Red Teaming festgelegt?

- Die Ziele werden in Abstimmung mit dem Kunden festgelegt und sind je nach Unternehmen und dessen Sektor individuell. Die Ziele sind kundenabhängig.
- Als Ziel wird festgelegt an die „Kronjuwelen", z. B. sensible Daten eines Unternehmens oder unternehmenskritische Systeme zu kommen. Einzelne Systeme sind meistens nicht das Ziel, sondern das AD oder die Benutzer. Die „Kronjuwelen" werden zusammen mit dem Management oder Sicherheitsverantwortlichen bestimmt und daraus ein Ziel formuliert.
- Um ein Ziel festzulegen sollte hinterfragt werden, was die wichtigen Prozesse im Unternehmen sind, was geschützt werden muss und welche Möglichkeiten es gibt diese anzugreifen. Was sind die schützenswerten Daten im Unternehmen?
- Bei der Zielbestimmung geht das Unternehmen in die Rolle des Angreifers und schaut, was das Schlimmste wäre was passieren könnte. Daraus werden die Ziele abgeleitet.
- Das Unternehmen sollte die Ziele vorgeben. Da dies das Unternehmen nicht immer können, wurden Vorschläge gemacht und mit dem Unternehmen besprochen. Die Vorschläge können gemacht werden, aber das Unternehmen muss die Ziele festlegen. Die Ziele werden auf Grundlage von Rückfragen erörtert.
- Das Ziel kommt häufig aus dem Business Continuity Management. Die zentrale Fragestellung zum finden des Ziels ist: „Was tut dem Unternehmen besonders weh?" Ein Ziel kann auch nicht-technisch mit einen große Business Impact für ein Unternehmen sein.
- Über die Ängste des Kunden, werden mögliche Ziele ausgemacht. Bei den Gesprächen wird auch bspw. nach Bereichen, die nicht angegriffen werden können, gefragt, um die als mögliches Ziel zu Identifizieren.
- Beispiele:
    - In einem Krankenhaus ist ein Kernprozess die Versorgung der Patienten und es muss jederzeit möglich sein die Patienten zu behandeln. Dort gibt es auch Schwerpunktzentren und kritische Stationen, die besonders geschützt werden müssen. Dies kann ein Ziel sein.
    - Zugriff auf ein bestimmtes System.
    - Auf sensible Daten vom SAP-System zugreifen.
    - Extrahieren von Forschungsdaten in einem abgesicherten Bereich kommen.
    - Die E-Mails des Vorstands abzurufen.
    - Administrative oder Domain-Administrator-Rechte zu erhalten.
    - An Informationen, Daten, Benutzer und Unternehmensbereiche zu kommen.
    - Eine Anwendung, Datenbank, bestimmte Benutzer oder Personaldaten.
    - Konstruktionsdaten auszulesen.
    - Schutz vor Malware oder Ransomware.

    - Zugriff auf ein bestimmtes Netzwerksegment mit kritischen Systemen zu kommen.
    - Bei kritischen Infrastrukturen, Nuklear Sektor oder Unternehmen bei den Maschinen betrieben werden, geht es häufig darum eine Infrastruktur bspw. eine Maschine zu kontrollieren.
    - Privilege Escalation von einem bestimmten System ausgehend.
    - Wird das Erstellen eines Domainadministrators erkannt?
    - Wird das starten von einen Schwachstellenscan (Nessus, OpenVAS) in einem internen Netzwerk erkannt?
    - Von außen in ein Unternehmen einzudringen.
    - Baupläne die nicht in die Hände Dritter kommen dürfen.
    - Abfotografieren einer Produktionsanlage.
    - Zugriff in einem Rechenzentrum.
    - Unterlagen aus einer bestimmten Abteilung, z. B. der Abteilung vom Chef sein (ein Business Asset).
- Wichtig ist zu beachten, dass ein echter Angriff unter Umständen gar kein Domain-Admin benötigt, sondern über eine bestimmte Funktion oder Account an sein Ziel kommen kann. Ein Ziel kann es sein, ein Domain-Administrator zu erhalten. Bei anderen Unternehmen ist ein Domain-Administrator nicht als kritisch anzusehen.

3. Ablauf / Prozess- Wie läuft ein Red Teaming ab?

Vorbereitung

- Von einem Auftraggeber wird festgelegt, dass ein Bedarf für eine Analyse besteht. Dies kann intrinsische Motivation der Organisation oder durch Regularien vorgeschrieben sein.
- Der CISO schreibt einen Auftrag an das Red Team und informiert das White Team. Das White Team ist oft der Leiter des Red Teams. Das White Team koordiniert und kontrolliert den Test.
- Die beauftragt erfolgt von der Business-Seite. In der Regel dem Management.
- Beim Dienstleister wird tlw. das CERT und der Sicherheitsbeauftragte über den Test informiert. Es gibt Tests, bei dem die Verteidigung informiert wurde und welche ohne Informationen.
- Zum Teil werden Ausschlusszeiten festgelegt, um sensible Betriebsabläufe in einer Universität oder einem Krankenhaus nicht zu stören.
- Es ist wichtig datenschutzrechtliche Vorgaben zu beachten. Es gibt eigene Rechtsberatung aus Juristen, die bei Datenschutzfragen hinzugezogen werden können.
- Das Projekt startet mit einem Workshop, der in der Regel ein oder zwei Tage dauert. Bei diesem Workshop werden die Dos and Don’ts, die Kronjuwelen, das Vorgehen, die Risiken und Szenarien besprochen.

- Zu Beginn gibt es eine Besprechung mit dem Red Team, ein Scope und das Engagement festgelegt bzw. der Rahmen definiert. Es wird vereinbart, was gemacht werden darf und was nicht (z. B. Brute-Force, Password-Spraying). Im Anschluss gibt es einen Auftrag.
- An Anfang erfolgt eine Abstimmung mit dem Kunden, was getan werden soll, wo angefangen wird. Ein Beispiel kann ein Außentäter oder ein Innentäter, der bereits ein kompromittiertes Gerät hat.
- Ein Red Teaming startet mit einer Anfrage vom Kunden und einem darauffolgende Kundenmeeting (häufig telefonisch) bei dem der Bedarf erläutert wird.
- Nach der Anfrage kommt es zu einem Kick-of-Gespräch. Dies ist der Einstieg beidem herausgefunden werden soll, was das Unternehmen möchte. Hierbei geht es darum, ob ein Pentest oder ein Red Teaming benötigt wird. Die Gespräche werden bspw. mit einem CISO geführt, der die Security-Level des Unternehmens testen möchte. Weitere Fragestellungen:
    - Wurde so etwas schonmal durchgeführt?
    - Was ist Red Teaming (Aufklärung)?
    - Sind die Mitarbeiter bereits für Phishing sensibilisiert?
    - Gibt es Security Awareness Maßnahmen?
- Der Scope wird im Auftaktgespräch in Absprache mit dem Kunden festlegen.
- Anschließend folgt die Angebots- und Vertragserstellung.
- Ein Projekt startet mit einem Erstgespräch beidem geklärt wird, ob Red Teaming für den Kunden die richtige Methodik ist. Im Gespräch wird der Ansprechpartner identifiziert und anschließend ein Angebot erstellt. Diese ist Vertrauensperson des Unternehmens. In den Gesprächen werden die Ziele und Interessen des Unternehmens besprochen. Auch ISMS und eingesetzte Standards werden betrachtet. Die Planung wird in Abstimmung mit dem Ansprechpartner erstellt. Hier werden die relevanten Angriffsszenarien präzisiert und ausgewählt.
- Im Kick-Off-Meeting kommt es zur Abgrenzung, welche Angriffsmethoden eingesetzt werden dürfen.
- Wenn eine Anfrage des Kunden kommt, muss oft erst geklärt werden was Red Teaming ist. Hierbei wird tlw. herausgefunden, dass ein Red Teaming kein Sinn macht und ein Szenario basierter Test nützlicher wäre.
- Das Projekt startet mit der Kontaktaufnahme und wenn ein Auftrag zustande kommt folgt ein Kick-Off.
- Im Vergleich zu vielen anderen Marktteilnehmern wird ein ausführliches Vorgespräch durchgeführt. Hier wird genau bestimmt, was der Kunde will, was ein Red Teaming ist und eine Abgrenzung zu anderen Methoden verdeutlicht. In der Vorabberatung wird auch geklärt was sinnvoll und beachtet werden muss.
- Bei Projektbeginn werden Meilensteine abgestimmt, bspw. in welcher Frequenz oder nach welchen Zielen kommuniziert wird, ob ein System übernommen werden darf.
- Beim Red Teaming wird ein „Playbook“ erstellt, dass die Vorgehensweise, Meilensteine, Zeitpunkt etc. beschreibt.

- Es gibt auch eine grobe Abstimmung über die Vorgehensweise. Diese wird nicht geheim gehalten.
- Die festgelegten Regeln werden in Abstimmung mit dem Kunden in einen Vertrag gegossen.
- Phasen in einem Red Teaming sind analog zum TIBER-EU Framework: Scenario Planning > Preparation > Attack > Persist > End Exercises > Analysis > Report

Durchführung

- Bei einem Social Engineering werden Informationen gesammelt und eine Phishing Angriff vorberietet.
- Die Vorgehensweise ist wie in einer üblichen Kill Chain im Unterschied zum Penetrationstest möchte man bei einem Red Teaming nicht erkannt werden.
- In der Vorbereitungsphase werden Informationen über das Unternehmen gesammelt und Angriff als Proof-of-Concept auszuführen. In Krankenhäuser ist es häufig schwierig ein PoC auszuführen, daher geht es nur bis zu der Stelle, dass ein Kompromittierung möglich wäre. Tests werden anschließend falls vorhanden in einem Testsystem durchgeführt.
- Kritische System können nicht im Live-Betrieb getestet werden. Hier wird auf Testsysteme ausgewichen.
- Bei der Durchführung gibt es keinen vorgefertigten Ablauf, sondern dies ist sehr abhängig von dem mit dem Kunden vereinbarten Ziel. Zum Start werden Informationen gesammelt. Das Vorgehen ist schrittweise und es wird abgesprochen, was wie lief und was besser gemacht werden könnte.
- Der Angriff startet immer mit einer Aufklärungsphase / Reconnaissance. Auf Grundlage von OSSINT, sozialen Netzwerken und öffentlichen Quellen werden Daten über den Auftraggeber gesammelt.
- In der OSINT-Phase werden Informationen über Partner, Dienstleister und externe Firma gesucht. Anschließend werden bspw. Verkleidungen, vorbereitet. Es gibt ein Set von Hilfsmittel, wie Kameras, Lock-Picking-Werkzeug usw. Zudem werden auch Mitarbeiterausweise, Visitenkarten, Blöcke, u.v.m. für einen Angriff vorbereitet.
- In der OSINT-Phase werden Daten über das Unternehmen gesammelt. Hierbei geht es darum Zusammenhänge auch zu Dritten herauszufinden und zu verstehen, sowie Daten aus Sozialen Netzwerken und öffentlichen Quellen zu sammeln. Auf Grundlage der OSINT-Phase wird ein Red Team Testplan erstellt. Der Testplan wird mit dem Auftraggeber abgestimmt. Hier werden die Tests abgestimmt.
- Die Durchführung startet mit einem Information Gathering, d. h. es werden Informationen über das Unternehmen gesammelt. Darüber sollen Angriffswege und Informationen für das Social Engineering gesammelt werden.
- Um in ein Unternehmen zu kommen wird Social Engineering, physische Angriffe und technische Angriffe unternommen. Bei physischen Angriffen wird bspw. durch Tailgating

ins Unternehmen eingestiegen und Netzwerk Implantate hinterlegt, mit deren Hilfe eine Verbindung nach außen aufgebaut wird.

- Während der Arbeit wird ständig eine Risikoanalyse, gemacht und hinterfragt, welche Konsequenzen ein Angriff haben kann. Die durchgeführten Angriffe sind wohlüberlegt und mit dem Auftraggeber abgestimmt.
- Ziel bei einem Angriff ist es möglichst unauffällig zu bleiben, d. h. einen möglichst „leisen" Weg zu gehen.
- Jeder Schritt wird beim Red Team zur Nachvollziehbarkeit dokumentiert.
- Das Projekt erfolgt tlw. stufenweise, d. h. wenn eine bestimmte Stufe erreicht wird, werden zuerst die Maßnahmen umgesetzt. Anschließend wird nachgeprüft und anschließend von einem gesonderten Zugang weiter getestet.
- Es gibt auch Kunden, die kein Phishing wollen.
- Sobald ein Zugriff von außen ins Unternehmen vorhanden ist, wird versucht die Verbindung zu persistieren. Das infizierte System wird anschließend getestet, um bspw. einen lokalen Administrator zu erhalten, den Autostart anzupassen, Services zu ändern, usw. Hier wird ebenfalls versucht möglichst unauffällig vorzugehen, aber auch getestet, ob eine Änderung vom Blue Team erkannt wird. Das infizierte System ist der Zugangspunkt zum Netzwerk. Von hier aus wird versucht auf weitere Geräte zu kommen.
- Beim System werden auch eingebundene Samba-Shares geprüft. Hierbei werden häufig Passwörter in Skript, Text, Log-Daten oder sonstige sensible Informationen gefunden.
- Auf dem Gerät wird auch versucht Endpoint-Lösung zu umgehen. Dabei soll ebenfalls versucht, werden, ob die Versuche erkannt werden. Diese Tests werden genau geplant, abgestimmt und genau ausgeführt, um mögliche Schwächen einer Lösung aufzudecken.
- Die Vorgehensweise ist in Phasen unterteilt die jeweils Meilensteine / Checkpoints haben. Für jede Phase ist eine maximale Zeit festgelegt. Wenn in einer Phase kein erfolgreicher Angriff möglich ist, wird in eine nächste Phase übergegangen.
- Das Red Team wird stufenweise in Abstimmung mit dem White Team durchgeführt.
- Wenn ein Ziel von einem Red Teaming frühzeitig erreicht wird, wir das Red Teaming „neugestartet" und über einen anderen Weg versucht ins Unternehmen zu kommen. Nach jeder Iteration ist die Vorgehensweise „lauter", d. h. es wird bspw. ein Portscanner eingesetzt und geprüft, ob dieser erkannt wird.
- An einem Test wird häufig durchgehend gearbeitet. Die Angriffe erfolgen nach der Abstimmung mit dem Auftraggeber.
- Beim Red Teaming wird jeder Schritt dokumentiert, sodass bei einem erfolgreichen Angriff der Pfad erkennbar ist und herausgefunden werden kann, wann was zu erkennen ist.
- Es wird ein detaillierter Bericht erstellt, der üblicherweise an das Blue Team geht. Die soll durch den Bericht die durchgeführten Schritte nachvollziehen können. Erfolgreiche Angriffe, sollen über Log-Daten nachgeprüft werden, ob diese erkannt werden hätte können und nach Möglichkeiten gesucht, wie diese in Zukunft erkannt werden.

- Der Bericht beschreibt detailliert den Tagesablauf und Angriffswege (Attack Path) und welche Angriffe erfolgreich waren.
- Anschließend geht es um das Bereitstellen von einem Schadcode der bspw. für eine Phishing Angriff benötigt wird. Die Phishing E-Mail wird auf Grundlage der gesammelten Informationen entwickelt.
- Danach geht es darum den Schadcode ins Unternehmen einzubringen, mit der Hoffnung, dass es von einem Mitarbeiter ausgeführt wird.
- Wenn der Schadcode ausgeführt wurde kommt es zum Command & Control.
- Mit der ausgeführten Malware wird die Kontrolle übernommen und versucht Tools nachzuladen, um sich zu persistieren und von dort aus weiter zu kommen.
- Die Prozesse können als „Reinkommen", „Drinbleiben" und „Ausführen" beschrieben werden. Alle Prozesse sind dazu da ein Ziel zu erreichen.
- Wenn eine freie Wahl der Angriffsvektoren möglich ist, wird zuerst versucht auf technischen Weg ins Unternehmen, anschließend über Social Engineering und erst dann auf physischem Weg.
- Die Durchführungsphase beginnt mit einer Internetrecherche und der Suche nach IP-Adressen/-Ranges. Die möglichen Ziele werden mit dem Kunden abgestimmt und diese müssen vom Kunden bestätigt werden. Anschließend werden die gefundenen Systeme in der Regel per Portscan geprüft. Dieser wird erst unauffällig und anschließend auffälligere Portscan. Dabei wird auch geprüft, ob ein Scan erkannt wird.
- Die erreichbaren Systeme und Dienste werden genau betrachtet (z. B. Outlook-Web-App, VPN-Zugänge).
- Auf die Login-Seiten werden Brute-Force-Angriffe durchgeführt.
- Wenn man einen Weg ins Unternehmen gefunden hat, wird versucht sich zu persistieren, die Rechte zu eskalieren bis ein Ziel erreicht wird.
- Es werden auch „Feuer" gelegt, um das Blue Team herauszufordern.
- Die höchste Erkennungsstufe sind Schwachstellenscans (z. B. Nessus, OpenVAS). Wenn dieser nicht erkannt wird ist dringender Handlungsbedarf notwendig.
- Wenn bspw. eine Jenkins Schwachstelle bekannt wird, werden die Jenkins Server geprüft und versucht die Schwachstelle auszunutzen und bspw. an die Daten in der Datenbank zu kommen. Eine bekannte Schwachstelle wird als Incident bewertet. Es wird versucht proaktiv Schwachstellen auszunutzen und Maßnahmen einzurichten.

Abschluss

- Über den Test wird ein Abschlussbericht erstellt. Dieser wird den Testverantwortlichen, dem Blue Team und dem Vorstand präsentiert.
- Die Ergebnisse werden ausgewertet und dem Auftraggeber präsentiert.
- Im Test wird eine Dokumentation erstellt und mit Abschluss des Tests präsentiert. Dies ist in der Regel eine Präsentation oder Workshop mit der IT-Security Abteilung. In diesem Termin werden auch Maßnahmen besprochen. Um diese im Nachgang zu testen, werden zum Teil noch gezielte Angriffe gefahren.

- Es werden im Nachgang tlw. Workshops mit dem Blue Team durchgeführt wie ein Logging verbessert werden könnte und Angriffe erkannt werden können.
- Nach der Abschlussbesprechung wird tlw. auch ein Training durchgeführt.
- Im Nachgang führt der Kunde aufgrund der Empfehlungen Implementierungen durch.
- Red Teaming kann auch zum Anlass genommen werden, weitere Security Awareness Maßnahmen im Unternehmen durchzuführen. Ein Beispiel hierfür wäre eine USB-Stick-Kampagne, bei der USB-Sticks bspw. auf einem Parkplatz verteilt werden, um getestet, wie oft die Sticks eingesteckt werden. Hiermit kann geprüft werden, ob das Unternehmen auf diese Weise tatsächlich angreifbar wäre.
- Es wird ein Ergebnisbericht geschrieben und den Teilnehmern präsentiert. Die Teilnehmergruppe wird vom Auftraggeber festgelegt. Häufig ist es ein CISO und ein Vertreter aus der Führungsriege.
- Im Report wurde beschrieben, was gemacht wurde. Anschließend erfolgt ein Briefing / Abschlussgespräch. Wichtig war die Zeitleiste, wann welcher Angriff durchgeführt wurde.
- Beim Abschlussgespräch wurden alle „Teile einer Kette“ eingeladen, d. h. auch bspw. Application Owner und Entwickler.
- Nach dem Test gab es meistens sehr viele Action-Items die abgebarbeitet werden mussten.
- Es ist häufig ein Sicherheitskonzept vorhanden, aber das Incident Handling, die Erkennung von Angriffen und die Reaktion darauf noch nicht ausgeprägt. Dies kann ein Ergebnis aus dem Red Teaming sein.
- Bei den ersten Tests war die Kommunikation zwischen Red, White und Blue Team noch schwierig und nicht alles nachvollziehbar, weil es keine komplette Offenlegung zwischen den Schritten des Red und Blue Teams gibt. Dies hat sich mittlerweile verbessert und wird weiter optimiert.
- Es wird geprüft, was aufgeklärt wurde, wo die Schwachstellen liegen und an was es gelegen hat.
- Danach setzt man sich zusammen und bespricht, was gut und was schlecht gelaufen ist.
- Die meisten ausgenutzten Schwachstellen beruhen auf Fehlkonfigurationen und ungepatchten Systemen.

Dauer / Anzahl Mitarbeiter

- Die Dauer von einem Projekt ist sehr abhängig vom Scope.
- Ein Angriff Vorort ist kürzer als ein technischer Angriff von außen.
- Im ersten Gespräch wird auch abgestimmt, wie lange ein Projekt laufen soll
- Die Dauer variiert zwischen 2 – 4 Wochen.
- In einem Projekt arbeiten typischerweise zwei bis drei Mitarbeiter und es dauert 4 Wochen bis 6 Monate. Dies ist abhängig vom Kunden.
- Das Team besteht aus mehreren Personen. Es sind mind. 2 Person und häufig 3-4 Mitarbeiter.

- Die Dauer kann sehr unterschiedlich sein. Der Durchschnitt liegt bei ca. 60 Tage. Diese Tage beinhalten den kompletten Ablauf und das Projektmanagement. Nach oben hin sind bei einem Red Teaming häufig keine Grenzen gesetzt.
- Unter den Mitarbeiter gibt es unterschiedlichen Fokuspunkten. Einer kümmert sich bspw. um die Generierung von Wissen aus den gesammelten Daten. Eine weitere Person kennt sich gut mit Antivirus-Evasion.
- Ein Red Teaming sollte mind. ein Quartal lang dauert.
- Die Dauer von einem solchen Test ist sehr unterschiedlich und lieg häufig zwischen 15 und 60 Tagen. Die Angriffspfade werden mit dem Auftraggeber abgestimmt. Es werden daher in der Regel nicht alle Angriffspfade getestet. Wenn ein Ziel früher erreicht wird, werden anschließend noch weitere Wege versucht oder die Tests ergänzt bspw. durch einen Whitebox-Test der physischen Infrastruktur. Bei jedem Assessment ist eine Zeit Vorort eingeplant indem ebenfalls Informationen über die Infrastruktur gesammelt werden.
- Ein Projekt dauert ca. 10 bis 28 Personentagen.
- Das Team besteht aus zwei Mitarbeitern. Bei Bedarf werden Spezialisten aus unterschiedlichen Bereichen hinzugezogen.
- Ein Red Teaming ist länger als ein Penetrationstests. Durchschnittlich dauert es nach seiner Erfahrung 14 Tage. In einem Team sind 2 bis 3 Mitarbeiter.
- Ein Projekt dauert zwischen 15 und 30 Personentagen.
- Die Teamgröße ist abhängig vom Projekt und kann von einer bis zu sieben Personen sein. Einzelne Personen sind auf bestimmte Spezialgebiete spezialisiert und können hinzugezogen werden.
- Beim Red Teaming waren 4 Personen Vollzeit ein halbes Jahr beauftragt.
- Die Dauer richtet sich nach dem festgelegten Budget.
- Die Infrastruktur für ein Red Teaming wie ein C&C-Server aufzubauen hat immer sehr viel Zeit in Anspruch genommen.
- Die Planung der Vorgehensweise („Playbook“) hat ebenfalls sehr zeitintensiv.
- Für das Red Teaming wurde ein Team von mehreren Personen beauftragt.
- Die Planung ist wesentlich umfangreicher als bei einem Penetrationstest.
- Red Teaming ist in der Regel dann abgeschlossen, wenn das Ziel erreicht wurde.
- Die Dauer der Projekte war unterschiedlich. Von Projekten die etwa 8 Wochen dauerten, bis zu einem Projekt das 6 Monate permanent lief. Tlw. werden die Tests dauerhaft immer in einem bestimmten Quartal z. B. 2 Wochen durchgeführt.
- Die Dauer von einem Red Teaming Projekt liegt zwischen 40 und 80 Personentagen.
- Ein Team besteht meistens aus 2 Mitarbeiter. Dies wird als gutes Maß angesehen. Bei Bedarf werden noch weitere Experten hinzugezogen (z. B. Experten für Windows- / SAP)
- Beim Team können je nach Phase Mitarbeiter hinzugeholt werden. Es gibt immer mehrerer die das ganze Projekt komplett begleiten und manche die nur in bestimmten Phasen unterstützen.
- Ein Team besteht aus 3 bis 7 Testern.

- Ein Projekt läuft ca. 6 Monate.
- Es kümmern sich drei Mitarbeiter um Red Teaming im Unternehmen. Das Team wird durch Zuarbeiten von weiteren Mitarbeitern zum Teil erweitert. Es erfolgt eine enge Abstimmung mit internen IT-Abteilungen. Es wird mit internem Knowhow gearbeitet.
- Banken haben baue zum Teil ein eigenes Red Team auf und führen Red Teaming kontinuierlich bzw. einmal im Quartal durchzuführen.
- Ein Projekt dauert 6 bis 9 Wochen und es gibt zwei aktive Mitarbeiter im Red Team.

Kommunikation

- Die Anzahl der Kommunikation ist unterschiedlich. Bei manchen gibt es tägliches Status-Updates, häufig läuft dies aber nach Bedarf.
- Es gibt eine Telefonnummer, die dem Auftraggeber übergeben wird, an die er sich bei Problemen wenden kann.
- Während des Tests gibt es nach jeder Phase oder individuell vereinbarte Zwischenmeetings.
- Der Zyklus der Abstimmung mit dem Kunden ist sehr unterschiedlich. Manche möchten ein tägliches Statusmeeting und manche wöchentlich. Es erfolgt eine Abstimmung zwischen jeder Phase.
- Es gibt eine tägliche Abstimmung über die Vorgehensweise mit dem Auftraggeber.
- Es gibt meistens einen täglichen Status-Call.
- Der Ansprechpartner im Unternehmen wird in der Regel auf dem Laufenden gehalten. Das Blue Team ist nicht über einen Angriff informiert.
- Je nach Kundenwunsch wird, das Blue Team darüber informiert, was genau gemacht wurde.
- Die Kommunikation zwischen dem Dienstleister und dem Auftraggeber ist sehr unterschiedlich. Ein Red Teaming wird manchmal sehr offen im Unternehmen kommunizier und tlw. nicht.
- Die Kommunikation zwischen Auftraggeber war sehr unterschiedlich von keiner Kommunikation bis zur täglichen Kommunikation. Das gebräuchlichste ist ein Wochenmeeting. Die Zeitfenster und Feedbackloops hatten somit unterschiedliche Frequenz. Wie beim Penetrationstest gibt es ein Kick-off und Zwischenfeedbacks.
- Die Eskalationsstufen wurden festgelegt.
- Es gibt regelmäßige Abstimmungen mit dem Kunden. Hier wird bspw. eine Liste mit gefundenen IP-Adressen abgestimmt, um herauszufinden, ob das dahinterliegende System zum Unternehmen gehört. Hier ist auch wichtig zu beachten, dass unter Umständen Fremdfirmen informiert werden müssen, wenn diese ein System betreiben. Hierbei wird eine schriftliche Bestätigung angefordert. Die Erfahrung ist, dass die kritischen Systeme meistens im Netzwerk des Kunden stehen.
- Die Status-Calls und regelmäßige Kommunikation sehr wichtig für den Erfolg des Projekts.

- Kommunikation: Kommt auf den Kunden an. Der Kunde bekommt einen Status bei einem Zwischenfall. Es wird auf die wichtigsten Punkte realisiert. In der Regel nur bei einem Milestone und auf minimale Punkte reduziert.
- Die Kommunikation erfolgt vom Red zum White Team. Das Blue Team kann beim White Team anfragen, ob es nur ein Test ist.
- Damit das Blue Team nachfragen kann, ob es sich um einen realen Angriff oder dem Red Teaming handelt ist tlw. der CISO informiert und es gibt eine Telefonnummer, wo dies erfragt werden kann.

4. Technik / Werkzeuge - Welche TTPs (Tactics, Techniques and Procedures (TTPs)), Methoden und Software werden verwendet?

Anteil technisch, physisch, Social Engineering

- In den Projekten wurde zu 90 % auf technischen Weg ins Unternehmen zu kommen und zu 10 % über Social Engineering Methoden wie Phishing und Tailgating. Viele Projekte werden ohne Social Engineering durchgeführt. Erfolgreiche Angriffe durch Social Engineering sind nur schwierig zu behandeln.
- Bei den Angriffen wurde zu 35 % Social Engineering (Phishing), 15 % Webanwendung, 30 % Social Engineering (Tailgating) und 20 % Physical Assessment verwendet.
- Die Angriffsarten bei den Aufträgen war zu einem Drittel per Phishing / physisch / technisch.
- Bei Red Teaming wird sehr viel öfter Social Engineering oder der Physische anstatt des technischen Wegs gewählt.
- Als Angriffsform wird häufig auf Social Engineering (Phishing oder physisch). Über öffentlich verwundbare Parameter und auf technischem Weg Zugang ins Unternehmen zu bekommen ist sehr selten.
- Je nach Projektzeit und Abstimmung mit dem Kunden werden auch unterschiedliche Angriffsvektoren verwendet.
- In Awareness-Schulungen werden die Ergebnisse und Erkenntnisse angesprochen und auf wichtige Aspekte hingewiesen.
- Es wird kein Physical Assessment und personelle Absicherungen durchgeführt, da dies von einem anderen Bereich betreut wird. Eine Kombination von physischen, technischen und menschlichen (Social Engineering) ist für die Zukunft geplant.
- In den meisten Projekten reicht es aus über einen technischen Weg ins Unternehmen zu kommen.

Wie werden die Angriffe ausgewählt?

- Bei der Angriffsart ist vieles abhängig vom Kunden und eine Zeitfrage. Dies wird im Assessment festgelegt. Häufig werden unterschiedliche Wege versucht.
- Es ist kein Weg ins Unternehmen zu kommen ausgeschlossen. Dieser wird in der Planungsphase festgelegt.

- Viele Tests sind abhängig vom festgelegten Scope. Hier wird auch festgelegt, was passiert, wenn der erste Perimeter gebrochen wird.
- Im Normallfall werden nicht mehrere Wege gesucht, sondern der vielversprechendste Weg ausgenutzt. Es ist eher untypisch mehrere Wege zu gehen. Dies wird nur bei einer Beauftragung durchgeführt.
- Die TTPs sind von den Threat Model abhängig und der Infrastruktur.
- Die eingesetzten TTPs richten sich nach der Threat Intelligence.
- Die Angriffe ergeben sich aus den TTPs.
- Die eingesetzten TTPs richten sich nach dem Kunden und entstehen aus der OSINT-Phase und dem Testplan.
- Je nach Test wird ausgewählt welches Werkzeug weiterhilft.

Physical Assessment

- Generell kommt Red Teaming aus dem militärischen Bereich, daher sind physische Angriffe in diesem Zusammenhang durchaus übliche Praxis.
- Bei einem Full Scope Test kommt das Unternehmen zu 80 % mit einem physischen Angriff ins Unternehmen. Dies wird auch als die Vorgehensweise mit geringstem Aufwand angesehen.
- Lock-Picking wird häufig nur im Unternehmen für interne Türen, Bürotüren, Safes oder Rechenzentren eingesetzt.
- Lock-Picking wird nur sehr selten eingesetzt.
- Beim Physical Assessment wird das Unternehmen zuerst von außen kennen gelernt und ein Überblick verschafft. Hierzu werden Notizen gemacht und auf Regelmäßigkeiten untersucht. Es wird bspw. geprüft, wo die Menschen reinlaufen und welche Zugangswege es gibt. Gibt es einen Weg einfach in das Unternehmen zu laufen. Es wird auch passiv in einer Kantine gelauscht und Small Talk mit Mitarbeiter geführt, um so an Informationen zu kommen und erste Kontakte zu knüpfen. Diese können helfen, um ins Unternehmen zu kommen und sich auszubreiten. Eine einfache Möglichkeit bei großen Gebäuden ist es, sich unwissend zu stellen, bspw. mit der Aussage das man sich verlaufen hat. Können Sie mich reinlassen. Physical Assessment wird häufig in Kombination mit Social Engineering eingesetzt.
- Beim Physical Assessment wird Tailgating angewandt und eine passende Verkleidung gewählt. Es sind auch Werkzeuge für Lock-Picking vorhanden, allerdings wird dies in der Regel nicht benötigt. Anstatt Türen aufzubrechen, wird lieber versucht, bspw. durch einen internen Anruf an einen Schlüssel oder jemanden zu kommen, um eine Türe zu öffnen. Man kann sagen, dass beim Physical Assessment zu 90 % Tailgating erfolgreich ist.
- Bei einer Bank war ein Körperscanner im Einsatz. Dieser hat geprüft, ob der bei sich geführte Token mit der Körpergröße übereinstimmt. Dieser konnte mit einer Person mit ähnlicher Größe überlistet werden.

- Beim physischen Angriff wird typischerweise die Social Engineering Methode Tailgating angewendet. Hierzu wird eine angemessene Kleidung gewählt und sich als eine Person ausgegeben. Auch Wege über den Raucherbereich oder offene Türen wird gewählt. Lock-Picking wird nur in Abstimmung mit dem Kunden angewandt.
- Die zweit häufigste Variante sind physische Angriffe. Ein Beispiel war, dass sich die Tester als Fenster-Putz-Firma verkleidet haben und Ausweise von diesem Unternehmen kopiert und mitgebracht haben und so ins Unternehmen gekommen sind.
- Bei Red Teaming können auch physische Angriffe durchgeführt werden. Dies wird aber von diesem Dienstleister nicht gemacht. Es wurden bisher noch keine Skills in diesem Bericht aufgebaut und haben bisher keinen Schwerpunkt beim Dienstleister. Grund hierfür ist, dass die relevanten Threat Actors keinen physischen Angriff erfordern.
- Bei einem transparenten Physical Assessment wird eine Begehung gemacht. In einem normalen Physical Assessment wird die Social Engineering-Methode Tailgating angewendet.
- Das Unternehmen hat keine Expertise in physischen Angriffen, benötigt dies auch nicht und möchte dies auch nicht aufbauen. Es gibt kein Human Intelligence. Auch Tailgating wird nicht angewandt. Es gibt kein Threat Model beidem ein physischer Zugang notwendig wäre. Der einzige Grund physisch Vorort zu gehen wäre, wenn bspw. ein Login von einem WLAN gefunden wird oder zum Wardriving. Dieser wird auch als realitätsnah angesehen.

Technical Assessment

- Es wird in der Regel immer zuerst technische Angriffe versucht. Dabei wird großer Weg daraufgelegt, dass die Angriffe möglichst realistisch sind.
- Tlw. konnte auch auf technischem Weg bspw. Webseiten oder andere Geräte die bspw. mit der Shodan-Suchmaschine gefunden wurde eine Verbindung ins Unternehmen aufgebaut werden. Ein Beispiel ist eine Upload-Funktion bei der eine Malware hochgeladen werden kann oder eine Command-Execution-Schwachstelle, die es ermöglicht, über einen Befehl eine Verbindung aufzubauen. Das anschließend kompromittierte System steht häufig in einer DMZ, über die tlw. Verbindung ins Netzwerk aufgebaut werden konnte.
- Ein technischer Angriff ist mit einem wesentlich höheren Aufwand verbunden.
- Es wurden Pass-the-Hash-Angriff durchgeführt.
- Hauptaufgaben waren eine Malware zu verschleiern und das einschleusen.
- Es ging darum einen Überblick über die Benutzer, Rolle, Rechte und Systeme zu erhalten und an welchen Systemen ein Benutzer angemeldet war.

Social Engineering

- Die häufigste Art ins Unternehmen zu kommen ist ein Spear-Phishing-Angriff mit einer Malware.

- Das Spear-Phishing ist die am häufigsten und erfolgreichste Variante in ein Unternehmen zu kommen.
- Spear-Phishing ist eine häufige Methode, die von den Threat Actors eingesetzt wird, daher wird dies auch verwendet.
- Wenn ein Eindringen in Unternehmen nicht über physischen Weg möglich ist, wird auch Phishing eingesetzt. Es gibt auch Tests bei, der nur versucht werden soll auf technische Art und Weise ins Unternehmen zu kommen.
- Ein Phishing wird nur dann durchgeführt, wenn es eine Nachfrage vom Kunden gibt.
- Über Phishing in ein Unternehmen zu kommen wird fast immer versucht, da eine gut gemachte Phishing-E-Mail normalerweise nicht erkannt wird. Nach dem man per Phishing auf ein Zielsystem gekommen ist kommt man durch die Netzwerksegmentierung oft nicht weiter und man muss sich einen anderen Weg suchen. Zum Beispiel ein Gerät in ein Unternehmen einbringen.
- Das Spear-Phishing wird gezielt auf eine ausgewählte Personengruppe ausgeführt. Die Personengruppe wird durch das OSINT festgelegt. Ein Whitelisting von einer E-Mail wird nicht durchgeführt. Dies wird bei einer Phishing-Kampagne häufig gemacht. Es gibt zum Teil auch Vorschläge von ausgewählten Personen des Auftraggebers.
- Bei den Tests kann Phishing erlaubt oder ausgeschlossen werden. Wenn es erlaubt ist wird es auch versucht.
- Interessante Erkenntnis ist, dass eine weibliche Person mit viel Motivation im Social Engineering erfahrungsgemäß erfolgreicher ist als ein Mann.
- Tlw. muss ein Nutzer z. B. per Phishing dazu gebracht werden eine Malware auszuführen.
- Bei Phishing wird Spear-Phishing praktiziert. Es wird meistens zuerst bei einem Mitarbeiter versucht und anschließend zum nächsten übergegangen.
- Es kommt auch häufig vor, das Mitarbeiter angegriffen wurden und nichts davon mitbekommen haben.
- Bei Social Engineering wird versucht einen Mitarbeiter zu schützen indem kein Name, Uhrzeit oder Ort dokumentiert wird. Es soll nicht möglich sein, herauszufinden, wer es war. In der Dokumentation wird der Datenschutz beachtet.

Software / Hardware

- Die eingesetzte Software, Tools und Techniken sind abhängig von der vorgefundenen Infrastruktur.
- Die Tool-Umgebung ist sehr dynamisch und wird häufig modifiziert eingesetzt.
- Die eingesetzte Software ist sehr unterschiedlich. Es ist eine Mischung aus Eigenentwicklung und bekannten Frameworks, wie Metasploit, Cobalt, Armitage und Empire.
- Es werden Standardtools vom Betriebssystem, Eigenentwicklung, bei Windows viel Cobalt Strike verwendet, Lateral Movement kommt es auf die Umgebung an. Bei Windows wird bspw. RDP oder SMB genutzt, um weiterzukommen.

- Cobalt-Strike und Empire. Mit diesen Frameworks kann eine Malware-Implantat je nach Infrastruktur entwickelt werden.
- Es gibt eine sehr breite Palette an klassischen Prüfwerkzeugen aus dem Pentestbericht. Zusätzlich gibt es Hardware-Gimmicks, Rubber Duckey, Pown Lugs, Hardware, um Zugangskarten zu kopieren, Kameras mit Teleobjektiven.
- Zusätzlich gibt es Tools, um ein Social Engineering durchzuführen.
- Metasploit und Empire wird gar nicht eingesetzt.
- Beim Red Teaming geht es auch darum unsichtbar und unbemerkt zu bleiben. Dies ist am besten mit legitimierten Zugriffen, Admintools oder Tools die wie Admintools funktionieren möglich. Teilweise werden Admintools imitiert.
- Es wird häufig versucht mit Windows Bordmittel an Zugangsdaten zu kommen. Ziel ist es ohne Exploits auszukommen.
- Bei Red Teaming wird auf viel Windows Bordmittel zurückgegriffen, da diese von Virenscannern nicht erkannt werden. Um von einem System zum anderen zu kommen werden z. B. PsExec. Es wurde eine Expertise aufgebaut, um sich per Windows Bordmittel auszubreiten.
- Die eingesetzte Malware sind tlw. Eigenentwicklungen.
- Es werden öffentliche Tools, wie Cobalt Strike eingesetzt.
- Es gibt Skripte für einzelne Prüfungen.
- Die eingesetzten TTPs sind je Tester sehr unterschiedlich. Es wird bspw. ein Kali Linux eingesetzt.
- Manche Mitarbeiter haben eigenentwickelte Skripte. Je nach Testart werden unterschiedliche Tools eingesetzt. Es kann nmap und Nessus eingesetzt werden. Wenn es darum geht nicht sichtbar zu bleiben muss häufig auf diese Tools verzichtet werden.
- Cobalt Strike wird viel bei Red Teaming eingesetzt. Das Unternehmen verzichtet aber darauf.
- Für die Kommunikation nach außen wurde z. B. Cobalt Strike verwendet. Mit diesem Tool wurde verschlüsselt nach außen kommuniziert
- Für die Kommunikation werden Protokolle wie bspw. HTTPS und SSH verwendet.
- Tools: PowerSploit-Skript, viele Eigenentwicklungen (Outlook-Plugin / Malware), Mimikatz, Office-Makros, Cobalt Strike, Metasploit, PowerShell, …
- Frameworks wie Metasploit und Co. werden häufig sehr schnell erkannt. Antiviren-Hersteller sind so gut, dass diese nur schwierig umgangen werden können.
- Die Vorgehensweise der einzelnen Mitarbeiter ist individuell. Bspw. haben manche Mitarbeiter selbstentwickelte Tools.
- Viele Tester haben ihre eigene Vorgehensweise entwickelt und nutzen die für sich hilfreichen Werkzeuge.
- Die Vorgehensweise ist vom Kunden und Mitarbeiter abhängig.
- Die Software wird ständig weiterentwickelt. Dadurch ändern sich die eingesetzten Tools ebenfalls

Allgemeines

- Die Angriffe werden auch kombiniert und zusammenhängende Angriffe durchgeführt. Zum Beispiel wird ein physischer Angriff mit Phishing kombiniert. Es wird eine E-Mail an den Empfang geschickt und bspw. die Anmeldung der Handwerker, Aufzugsmechaniker, Klempner, oder ähnliches durchgeführt. Auf diesen Weg werden Fremdgeräte ins Unternehmen eingebracht. Hier werden auch Fotos als Beweis verschickt oder NTLM-Hashes oder ähnliches gestohlen.
- Es werden immer möglichst manuelle Prüfungen und keine automatisierten Tests durchgeführt, um verdeckt zu agieren. Standardisierte Testverfahren wollen vermieden werden.

5. Unterschiede - Wo liegt der Unterschiede von einem Red Teaming zu einem Penetrationstest oder Audit?

Allgemein

- Wenn eine Tür von einem Haus bei einem Pentest geprüft wird, würde der Pentester versuchen an der Tür des Hauses zur rütteln und die Tür einzutreten. Das Red Team schaut sich die Tür an, wirft aber lieber ein Stein in das Fenster nebendran und versucht so reinzukommen.
- Verbildlicht gesprochen wird bei einem Penetrationstest an Türen, Wände geklopft und geprüft, wie stabil eine Anwendung ist, bzw. welche Schwachstellen vorhanden sind. Dies ist sehr gut und notwendig. Es sorgt häufig, für eine wesentlich höhere Sicherheit einer Anwendung. Beim Red Teaming geht, weiter wie ein Penetrationstest und versucht über andere Wege an ein Ziel zu kommen. Hierbei wird bspw. auch beim Nachbar gefragt, ob er einen Schlüssel hat, ein Tunnel gegraben oder auf anderen Weg und andere Methoden einzusetzen. Es werden auch Wege hinein über die Periphere versucht.
- Eine SQL-Injection wird auch im Pentest gefunden. Was mit der SQL-Injection erreicht werden kann nicht. Beim Red Teaming wird eine SQL-Injection genutzt, um auf weitere Systeme zu kommen. Ein Red Teaming ist daher wesentlich realitätsnaher.
- Die Ergebnisse von einem Pentest und Red Teaming sind unterschiedlich.
- Ein Pentest ist eine Breitensuche und ein Red Teaming eine Tiefensuche.
- Beim Pentest ist der Auftraggeber über den Test informiert, beim Red Teaming nicht.
- Bei einem Penetrationstester und bei einem Red Team Tester sind sehr unterschiedliche Skillsets gefordert.
- Der Unterschied liegt in der Expertise, dem Scope und der Priorisierung.
- Penetrationstests sind wichtig und können nicht durch Red Teaming ersetzt werden. Die Methoden müssen Hand in Hand gehen.
- Wenn beim Pentest der Scope zu gering oder falsch gesetzt wird, werden Schwachstellen nicht gefunden. Der Scope wird aufgrund des Freiheitsgrades vom Red Team ausgewählt.
- Audit werden Konfiguration betrachtet.

- Es gibt Schwachstellen, die bei einem Penetrationstests als kritisch angesehen werden (bspw. XSS) und in einem Red Teaming, häufig nur eine geringe Bedeutung haben. Andere Schwachstellen (bspw. SQL-Injection) haben eine große Bedeutung, da diese unter Umständen einen Zugang zum Unternehmen ermöglichen.
- Das Red Teaming ist breitgefächerter als der Penetrationstests.
- Die Einstellung, das Mindset von einem Penetrationstester und einem Red Teamer ist unterschiedlich. Es kann sein, dass das Mindset eines Angreifers bei einem Pentester nicht ausgeprägt ist. Ein guter Pentester ist nicht gleich ein guter Red Teaming, tlw. ist dies auch schwierig umzusetzen, da ein Pentester anders denkt.
- Beim Red Teaming werden so wenig Personen wie möglich informiert. Die Verteidigung weiß nichts über einen Test. Im Vergleich dazu ist ein Penetrationstests ein angekündigter Test.
- Beim Penetrationstest werden einzelne Systeme und Netzübergänge auf Schwachstellen überprüft. Hierbei wird ein White-Box-Ansatz gewählt, d. h. der Tester kann auf Dokumentationen zugreifen. Die Tests erfolgen von außen nach innen. Die Tests können neben technischen Prüfungen auch Tests der Prozesse und Menschen sein.

Penetrationstest

- Durch einen Penetrationstest wird versucht möglichst viele Schwachstellen zu suchen, zu finden und zu beheben
- Ein Penetrationstest ist im Gegensatz zum Penetrationstest kein gezielter Angriff auf Geschäftsprozess oder das Kerngeschäft, sondern auf einzelne Assets.
- Wenn beim Pentest der Scope zu gering oder falsch gesetzt wird, werden Schwachstellen nicht gefunden. Der Scope wird aufgrund des Freiheitsgrades vom Red Team ausgewählt.
- Penetrationstest möglichst viele Schwachstellen zu finden
- Bei einem Penetrationstest liegt die Aufgabe darin, in einem eng gesteckten Fokus alle oder möglichst alle Schwachstellen von einem vorgeben Ziel zu finden.
- Beim Pentest sollen möglichst alle Schwachstellen finden. Es hat einen gewissen Vollständigkeitsanspruch und ist mehr in die Breite ausgelegt.
- Wer möglichst viele Schwachstellen aufdecken möchte sollte eher ein Security Assessment machen.
- Bei einem Penetrationstest wird eine Kernkomponente betrachtet, oft wenig realistisch betrachtet mit dem Ziel eine Kernaussage über die Sicherheit herauszukriegen.
- Ein Penetrationstest ist wesentlich fokussierter und genauer abgesprochen.
- Beim Penetrationstest können umfangreiche Scans (z. B. nmap) durchgeführt.
- Ein Pentest hat eine Restriktion im Scope.
- Bei einem Penetrationstest werden IP-Adressen tlw. auch Zugangsdaten ausgeben. Es werden Daten dir zur Durchführung eines Penetrationstests benötigt werden zur Verfügung gestellt. Das Ziel ist es möglichst alle/ viele Sicherheitslücken zu identifizieren.

- Im Vergleich zum Red Teaming steht der Fokus beim Penetrationstest in der Regel nicht auf Privilege Escalation und Lateral Movement.
- Ein Penetrationstest ist im Vergleich sehr isoliert. Es wird nur ein System oder ein Netzwerk und nicht das Gesamtkonzept bzw. die Gesamtumgebung betrachtet.
- Beim Penetrationstest wird ein Scope festgelegt, der in der Regel ein IT-Assets ist. Bei diesem wird versucht Sicherheitslücken und Risiken aufzudecken. Die Erkennung von Angriffen ist in der Regel nicht die Aufgabe des Penetrationstests.
- Beim Pentest sind es häufig technische Ziele.
- Beim Penetrationstest ist kein Rückkanal notwendig.
- Beim Pentesting wird ein bestimmtes Zielobjekt nach dem Kundenwunsch geprüft (z. B. mobile Applikation, Netzwerk, Webanwendung).

Red Teaming

- Beim Red Teaming ist es kein Ziel möglichst kritische oder viele Schwachstellen zu finden.
- Ein Red Teaming ist prozessual geprägt.
- Es existiert häufig ein Blue Team / SoC das verbessert werden soll.
- Beim Red Teaming geh es um die Erkennung und Reaktion der interne IT.
- Ein Red Teaming hat keinen Vollständigkeitsanspruch.
- Im Red Teaming sind oft große Freiheiten.
- Im Vergleich zum Pentest geht es nicht darum, alle Schwachstellen zu finden, sondern einen Weg zum Ziel.
- Beim Red Teaming ist ein Ziel nicht erkannt zu werden und sich zu persistieren im Gegensatz zum Pentest.
- Beim Red Teaming werden nur die Sachen angeschaut die interessant sind.
- Beim Red Teaming geht es um Privilegien Escalation, Lateral Movement und legitimierten Zugriff zu erhalten.
- Ein Angreifer beim Red Teaming hört auf, wenn er ein Ziel erreicht hat.
- Beim Red Teaming wird versucht möglichst tief ins Unternehmen zu kommen.
- Red Teaming konzentriert man sich auf sich auf die Prozeduren und es sorg für Awareness im Unternehmen an.
- Beim Red Teaming werden keine Informationen über Kunden oder Mitarbeiter zur Verfügung gestellt.
- Beim Red Teaming ist „der Weg das Ziel“, d. h. es geht darum Angriffswege zu erkennen. Es werden die PPTs des Kunden getestet (People, Processes, Technology)
- Der Einsatz der Tools unterscheidet sich, so wird bspw. beim Red Teaming in der Regel kein Nessus-Scan durchgeführt, da dieser schnell erkannt wird und beim Red Teaming versucht wird nicht entdeckt zu werden. RT Toolchain hat zusätzlich viele Tools zur Persistierung und C&C, die man meist nicht im Pentest braucht.
- Beim Red Teaming werden auch Social Engineering Techniken und die physische Sicherheit geprüft.

- Im Unterschied zum Penetrationstests, weiß die Verteidigung nichts vom Angriff. Zudem werden neben den IT-Systemen auch die Prozesse, physische Gebäude und Personen getestet.
- Beim Red Teaming geht es vielmehr darum die Prozesse und die Reaktion auf einen Angriff als ein einzelnes System zu testen.
- Beim Penetrationstest ist der Zeitraum der Testdurchführung für die Verteidigung bekannt.
- Viele Techniken und Tools unterscheiden sich, da man beim Red Teaming möglichst unauffällig bleiben möchte, können bspw. häufig keine Scans oder Brute-Force-Angriffe durchgeführt werden. Diese würden direkt auffallen.
- Der Zeitaufwand verschiebt sich auf andere Tasks. So ist bspw. für die Planungsphase, in der die OSINT und Testplan erstellt wird, viel Zeit investiert.
- Ein Red Teaming ist auf Geschäftsführungsebene angesiedelt.
- Die Angriffe von Red Teaming haben ein breiteren Scope als bei einem Penetrationstest.
- Red Teaming hat einen Einfluss auf die operationalen Prozesse im Unternehmen.
- Bei Red Teaming wird der eine Weg zum Ziel gesucht und wie ist man dort hinkommen kann.
- Beim Red Teaming wird auf ein goldenes Ziel hingearbeitet.
- Die Angriffe sollen häufig ein APT abbilden.
- Im Unterschied zum Pentesting sitzen beim Abschluss Gespräch häufig auch Application Owner und weitere Personen, die vom Angriff betroffen war, dabei.
- Beim Red Teaming geht es darum an die „Kronjuwelen“ zu kommen und in Netzwerksegmente von außen nach innen vorzudringen, sowie die Datenexfiltration ohne, dass man erkannt wird.
- Die Planung bei Red Teaming ist wesentlich aufwendiger – Infrastruktur bereitstellen, Domain registrieren, administrativer Aufwand für die Infrastruktur. Auch die Nachbereitung ist wesentlich aufwendiger, da alles sauber entfernt werden muss.
- Das Privilege Escalation steht bei Pentesting häufig nicht im Vordergrund.
- Beim Red Teaming werden explizit auch Exploits gebaut.
- Bei einem Red Teaming ist es nicht das Ziel alle Schwachstellen zu finden.
- Ein Red Teaming soll ein APT simulieren. Es geht darum kritische Schwachstellen zu finden, die für die Zielerreichung notwendig sind.

6. Gemeinsamkeiten - Was sind Gemeinsamkeiten von einem Red Teaming zu einem Penetrationstest oder Audit?

- Bei sehr kleineren Unternehmen und kritischen Infrastrukturen, beidem auf technischem Weg versucht wird ins Unternehmen zu kommen ist ein Penetrationstests häufig gleich wie Red Teaming. Hier fehlt häufig eine Netzwerksegmentierung, SoC und Awareness-Schulungen.
- Mit beiden Methoden wird versucht Schwachstellen aufzudecken.
- Es gibt einen Auftraggeber, der dies beauftragt.

- Die grundlegende Expertise der Prüfer ist gleich.
- Die Skills der Tester überschneiden sich zum Teil.
- Das Skill-Level der Tester ist ähnlich.
- Es werden bei beiden Methoden Reports geschrieben. Der Inhalt ist aber unterschiedlich.
- Ein Scope wird bei beiden Testweisen definiert.
- Das Red Teaming beinhaltet einen vollwertige Penetrationstest und gibt einen Einblick der Sicherheitsbelangen einer Infrastruktur.
- Die vom Kunden festgelegte Zeitdauer und Budget für die Ausführung kann ähnlich lang oder gleich sein.
- Der Übergang von einem Red Teaming zum Pentest kann fließend sein.

TTPs / Software

- Technisch gibt es sehr große Schnittmengen.
- Es gibt Überlappung der Software die eingesetzt, aber auch viele Unterschiede. So wird Cobalt Strike z. B. bei einem Penetrationstest nicht eingesetzt.
- Viele Tools können sowohl beim Red Teaming als auch beim Penetrationstests eingesetzt werden: Mimikatz, Responder, Cobalt Strike, Metasploit....
- Die Vorgehensweise, Prozess und Methodik ist grundsätzlich sehr ähnlich zum Penetrationstest.
- Beim Red Teaming werden auch Schwachstellenscans durchgeführt, um Schwachstellen zu finden. Bei manchen wird das Ziel unauffällig zu bleiben ausgegeben. Dies ist abhängig vom Kunden.
- Die Techniken, die sich beim Pentest bewährt haben, werden auch beim Red Teaming genutzt. Es werden viele gleiche Techniken und Methoden eingesetzt.
- Es geht darum Schwachstellen aufzudecken, es werden häufig gleiche Werkzeuge, Abläufe, Prozesse, Phasen durchlaufen. Die Tests haben viele Gemeinsamkeiten. Man könnte sagen, dass Red Teaming ein „Bruder“ vom Pentesting ist, da viele Teilaspekte beim Red Teaming Anwendung finden.
- Die eingesetzten Werkzeuge und Methoden sind sehr vergleichbar oder zum Teil dieselben.
- Phase der initialen Kompromittierung ist gleich.
- Beim Red Teaming werden auch Methoden und Techniken des Penetrationstest eingesetzt.
- Beide Methoden sind größtenteils technischer Natur.
- Die eingesetzten Mittel sind häufig die Gleichen.

7. Vorteile - Welche Vorteile hat ein Red Teaming? Warum sollten ein Unternehmen ein Red Teaming durchführen?

- Die Erkennung wird durch Red Teaming verbessert. Dies ist ein großes Defizit von vielen Unternehmen. Man kommt nicht gegen Zero Day Exploits und Phishing an und man kann

nicht alle Endpunkte prüfen, aber man sollte die Angriffe zeitnah erkennen. Der Fokus beim Red Teaming liegt auf der Detektion.

- Der größte Benefit ist es, das Blue Team zu stärken und herauszufordern, um die Reaktionsfähigkeit zu stärken.
- Es ist ein realitätsnaher Angriff, indem es darum geht Angriffe zu detektieren.
- Hauptaspekt war die festgelegten Sicherheitsmechanismen/ -maßnahmen des Blue Teams (SOC) zu prüfen.
- Ein Red Teaming ist ein sehr realitätsnaher Angriff. Dadurch werden viele unbewusste Schwachstellen aufgedeckt und behoben, was es einem Angreifer die Arbeit erschwert.
- Kunden nutzen ein Red Team, um mehr Budget für den Security Bereich zu erhalten.
- Es wird genutzt, um das Security Budget zu erweitert und festzustellen, wo mehr investiert werden muss.
- Aus den Ergebnissen kann abgeleitet und bewertet werden, ob das Budget sinnvoll eingesetzt wird.
- Das Red Teaming ist ein Training für das Blue Team.
- Red Teaming ist ein globaler Check, um an Schwachstellen zu kommen, die bei einem Penetrationstest unter Umständen nicht gefunden werden.
- Es werden Prozesse getestet. Zum Beispiel, wie gut das Incident Response funktioniert, ob Angriffe zurückverfolgt werden könne, welche Defizite die Prozesse haben und ob es Black Spots gibt.
- Die Schwachstellen können im Nachgang aufgearbeitet werden und Prozesse verbessert.
- Full Scope Red Teaming ist ein Test von Personen, Prozesse und Physische Sicherheit und nicht nur die technische Sichtweise.
- Es werden auch Personen und die Awareness geprüft.
- Die Auswirkung von einem von einem Security Breach wird veranschaulicht.
- Ein oder mehrere Angreifer Wege werden dargestellt.
- Es dient als Vergleich, wie man als Unternehmen dasteht.
- Der Business Fokus ist beim Red Teaming größer als beim Pentesting.
- Es wird auch die Reaktion von Mitarbeiter und dem Blue Team getestet.
- Durch Red Teaming kann eine Steigerung der Awareness erreicht werden.
- Red Teaming gibt häufig einen Überblick über alle relevanten Sicherheitsthemen.
- Es werden häufig die „größten“ / kritischen Schwachstellen aufgedeckt.
- Es dient als Training für das Blue Team.
- Das Red Teaming ist eine ganzheitliche Betrachtung eines Unternehmens. Es geht nicht um das identifizieren von kritischen Schwachstellen, sondern die ganzheitliche Sicherheit zu betrachtet. Im Test geht es darum zu prüfen, ob die notwendigen Sicherheitsmaßnahmen getroffen wurden.
- Es werden realitätsnahe Szenarien abgebildet und simuliert.
- Das Red Teaming betrifft die Prozessebene einer Organisation.

- Es war auch hilfreich, um neue Angriffe bzw. Angriffswerkzeuge auszuprobieren und zu prüfen, ob diese erkannt werden.
- Mit dem Test kann eine ganze Sicherheitskette geprüft werden.
- Hiermit kann simulieren werden wie die IT auf einen echten Angriff reagiert und Notfallprozeduren getestet werden.
- Interessant ist auch die Erkenntnis, ob eine IT-Abteilung in der Lage einen Angreifer „herauszuwerfen". Die IT ist tlw. damit überfordert Angreifer vollständig und nachhaltig zu entfernen.
- Ein Unternehmen kann auch herausfinden, ob ein Backdoor erkannt wird.
- Denkweise eines realen Angreifers wird simuliert.

8. Nachteile - Welche Nachteile hat die Durchführung eines Red Teaming?

Voraussetzungen

- Das Sicherheitskonzept sollte durch Penetrationstests und Security Awareness Maßnahmen bereits verbessert sein. Es sollte bereits ein hoher Reifegrad vorhanden sein.
- Ein Unternehmen sollte bereits einen möglichst hohen Reifegrad haben. Bei allen anderen Unternehmen ist der Mehrwert in der Regel gering und es wird dazu geraten Penetrationstests durchzuführen. Auch wenn ein Vulnerability Assessment oder Penetrationstest bereit Jahre zurückliegt empfiehlt sich eher ein Penetrationstest.
- Es lohnt sich erst ab einer bestimmten Größe.
- Ein Red Teaming bei einem kleinen Unternehmen würde wenig Sinn machen.
- Red Teaming ist nur sinnvoll, wenn die Strukturen, wie ein Blue Team vorhanden sind. Ansonst könne die Ressourcen besser eingesetzt werden.
- Die Unternehmen, die ein Red Teaming durchführen haben häufig bereits etliche Penetrationstest durchgeführt und keine Schwachstellen mehr gefunden. Das Red Teaming wird somit als nächste Stufe angesehen.
- Es ist sinnvoll zuerst einen bestimmten Reifegrad zu erreichen, z. B. durch den Aufbau eines Vulnerability Managements. Es muss zudem klar sein, ob und welches die „Kronjuwelen" sind. Dies kann bspw. ein Intellectual Property sein.
- Red Teaming wird dann gemacht, wenn das Geführt besteht, dass das Incident Response und die Sicherheitssysteme einen gewissen Reifegrad sichergestellt ist.

Herausforderungen

- Wenn Red Teaming nicht gut gemacht wird, dann verfliegen viele Vorteile. Es darf keine 0.8.15 Angriff sein, sondern es soll ein Hin und Her zwischen Red und Blue Team sein.
- Blue Team wird nur nach dem erkannt was man tut. Das Blue Team entwickelt sich nur weiter, wenn was Neues gemacht wird, nicht wenn immer wieder das gleiche gemacht wird. Es sollte ein Katz- und Maus Spiel sein. Red Teaming muss dem Blue Team gerichtet sein.

- Es ist sehr schwierig herauszufinden, wer wirklich ein guter Dienstleister ist, d. h. wer das Geld wert ist?
- Die Mitarbeiter sollten mit dem Thema vor einem Test vertraut gemacht werden und Security Awareness Maßnahmen ergriffen.
- Dadurch das beim Kunde Unklarheit über Red Teaming und Penetrationstests besteht, kommt es auch dazu das ein Kunde sich ein anderes Ergebnis verspricht, da er ein Penetrationstest erwartet. Bei Red Teaming kann auch die Schwachstelle Mensch ausgenutzt werden. Dadurch ergibt sich ein anderes Ergebnis. Dies muss im Vorfeld geklärt werden.
- Es muss klar geregelt werden, was ein Red Teaming kann und was nicht.
- Bei einem Test gibt es meistens sehr viele unterschiedliche Interessengruppen auf, die eingegangen werden, muss. Die Kommunikation ist eine Herausforderung bzw. schwieriger wie bei einem Penetrationstests, da es viele Personen gibt die „abgeholt" werden müssen.
- Es kann eine Herausforderung und großer Aufwand bedeuten, das Blue Team vom Red Teaming zu überzeugen. Sehr wichtig sind Workshops mit Blue Team im Nachgang zum Red Teaming.
- Die Auswirkung von einem Red Teaming sind häufig sehr stark, da die Tests in Abstimmung mit dem Vorstand durchgeführt werden. Es kam bspw. auf Grund des Tests große Investitionen in die IT-Sicherheit oder sogar Umbau an Fassaden oder Gebäude.

Nachteile

- Ein Red Teaming ist sehr teuer und zeitaufwendig.
- Ein Test ist sehr kosten- und zeitintensiv.
- Der Aufwand, Kosten und Dauer sind normalerweise wesentlich höher.
- Die Planung, Durchführung und Nachbereitung sind sehr aufwändig.
- Ein Red Teaming ist sehr teuer, aufwändig und es wird nicht nach rechts und links geschaut, sondern nur versucht ein festgelegtes Ziel zu erreichen
- Man versucht mit einem Weg ins Unternehmen zu kommen– Weitere Einstiegspunkte werden oft nicht geprüft und sind dann nicht im Fokus. Man bleibt häufig bei einem Einstiegspunkt.
- Ein Red Teaming dient nicht für ein initiales Assessment.
- Mit dem Red Teaming kann nicht die Fähigkeit des Blue Teams oder der Sicherheit bewertet werden. Es kann auch keine vernünftigen Aussagen über die Verteidigungsfähigkeiten geben, da ein Fehler reichen kann. Bei Red Teaming wird eine Schwachstelle gezielt ausgenutzt. Es können andere blinde Flecken überstehen werden. Man muss verstehen wie die Methodik funktioniert und was nicht damit erreicht werden kann.
- Beim Kunden sind viel Schwachstellen bereits bekannt und so kann es sein, dass ein Red Teaming nur wenige neue Erkenntnisse liefert.
- Es werden nicht einzelnen System ausführlich getestet.

- Es kann nur bewertet werden was gefunden wird.
- Nicht jeder Mitarbeiter finden einen Test gut. Ein Test kann für schlechte Stimmung im Unternehmen sorgen.
- Bei einem Red Teaming werden einzelne Schwachstellen ausgenutzt. Es können weitere kritische Schwachstellen unentdeckt bleiben.
- Dienstleister „hauen blind drauf". Dadurch entstehen Risiken und Schwachstellen bleiben unentdeckt.

Sonstiges

- Es bringt nur etwas, wenn aus dem Ergebnis gelernt wird und sich was daraus entwickelt.
- Ethischer Aspekt müssen beachtet werden.
- Der Dienstleister hat eine Ethik festgelegt, dass Mitarbeiter nur auf eine Art und Weise angegriffen werden dürfen, die tatsächlich ein Mitarbeiter erleben kann. Ein Wachmann darf bspw. nicht jeden reinlassen. Es kann aber durchaus vorkommen, dass sich jemand als jemand andere ausgibt. Ein weiteres Beispiel ist ein Phishing-Mail mit der ein Mitarbeiter rechnen muss. Es werden auch nur Angriffe durchgeführt, die einen Mehrwert haben.

9. Risiken - Welche Risiken hat die Durchführung eines Red Teaming?

Risiken physische Prüfungen

- Es kann zu Risiken für den Prüfer kommen, wenn diese zu blind vorgehen. Gewalttätigkeiten durch einen Sicherheitsdienst kann auch eine Gefahr für Leib und Leben oder eine Verhaftung zur Folge haben. Es ist ein sehr sensibles Vorgehen erforderlich.
- Es könnte theoretisch zu personellem Schaden des Testers bei einem Physical Assessment kommen, wenn bspw. bei einem Einbruch ein Wachschutz aggressiv reagieren würde. Dies ist aber noch nicht passiert.
- Es gibt ein höheres Risiko als beim Penetrationstests, da die Tests in Produktivumgebungen durchgeführt werden.

Risiken technische Prüfung

- Es gibt bisher keine kritischen Systemabstürze und größeren Schaden. Hierauf wird im Workshop auch explizit darauf hingewiesen, dass es dazu kommen kann. Beim Testen, wird auch versucht dies zu vermeiden indem bspw. bei kritischen Systemen erst nach Rückfrage ein Exploit ausgeführt wird.
- Bisher gab es keine größeren kritischen Ausfälle. Einzelne Systemabstürze sind durchaus üblich. Tlw. werden infizierte Rechner vom Blue Team eingezogen und die betroffen Person erhält einen neuen Rechner.

- Es gibt keine Erfahrung das ein kritisches System abgestürzt ist und es zu einem hohen Schaden gekommen ist. Bei kritischen Systemen wird auf Testsysteme ausgewichen.
- Bei den Tests kam es nicht zu großen Schäden.
- Es kam zu Systemabstürzen. Dies war eher beim Penetrationstests der Fall.
- Es kann zu Ausfällen kommen. Bisher gab es keine kritischen Ausfälle, da alles sehr genau geplant wird.
- Es gab keine größeren Ausfälle, die zu einem Schaden geführt haben.
- Es wurden Benutzer aktiv aus dem System geschmissen, um zu prüfen wie dieser darauf reagiert.
- Es kam zu Systemabstürze. Anschließend wurden Systeme neugestartet, um auch zu prüfen, ob diese erkannt werden.
- Es kann zu Systemabstürzen kommen.
- Es kann theoretisch zu Schäden und Ausfällen in einer Produktivumgebung kommen.
- Ein Red Teaming wird in Live-Produktivumgebungen durchgeführt, daher kann es zu Systemausfällen kommen.
- Da es ist ein realer Angriff ist kommt es auch zu Systemabstürzen und Angriff auf einzelne Personen.

Risiken Social Engineering

- Es können Risiken durch Social Engineering entstehen. Es kann durch Phishing herbe nachfolgen haben, so kam es vor das ein Mitarbeiter im Nachgang zu einer Phishing-Kampagne gekündigt hat.
- Auf ausgefallene Social Engineering Techniken fallen auch sehr geschulte Mitarbeiter rein.
- Das Social Engineering birgt das Risiko, das Mitarbeiter schlecht dastehen oder erniedrigt werden. Dies kann zur Unzufriedenheit in der Belegschaft führen, wenn sich Mitarbeiter ausgetrickst und vorgeführt fühlen.
- Es kann zu einer gewissen Unzufriedenheit kommen – tlw. fühlen sich Mitarbeiter hintergangen, weil sie nicht eingeweiht sind. Unternehmen sollte deeskalieren und darauf reagieren.
- Es kann zu Unzufriedenheit von Mitarbeitern, die sich durch einen Angriff kontrolliert fühlen.
- Bei Social Engineering Angriffen, kann das Vertrauen der Mitarbeiter an das Unternehmen in Mittleidenschaft gezogen werden. Dies ist aber auch abhängig von der Transparenz bzw. der Kommunikation im Unternehmen.
- Das Social Engineering kann zur Unzufriedenheit von Mitarbeiter führen und hat bereits dazu geführt das Mitarbeiter gekündigt haben. Es ist wichtig das die Mitarbeiter zum Thema Social Engineering geschult werden.
- Risiko: Eine erfolgreiche Phishing-E-Mail wurde im Unternehmen an alle Mitarbeiter weitergeleitet.
- Beim Social Engineering konnten keine negativen Beispiele gefunden werden.

- Es wurden bisher keine negativen Erfahrungen bezüglich Social Engineering Techniken gemacht.
- Das Risiko, das ein schwarzer Peter einer Person die einen Fehler gemacht hat, zugeschoben wird.

Lösungsvorschläge

- Es kam zu keinen negativen Erfahrungen bei den Social Engineering Tests. Interne Mitarbeiter erfahren auch häufig nicht, wann was passiert ist. Das Management verpflichtet sich, dass es keine Konsequenzen für einzelne Mitarbeiter gibt.
- Keine negative Erfahrung zu unzufriedenen Mitarbeitern oder Stabilität der Systeme. Man möchte nicht auffallen und gewissen Exploits werden nicht ausgenutzt, um möglichst die Availability nicht zu gefährden.
- Um eine bessere Akzeptanz bei den Mitarbeitern zu erreichen, ist die Empfehlung die Mitarbeiter darüber zu informieren, dass z. B. im Lauf des nächsten Jahres unangekündigte Tests durchgeführt werden können. Mit der minimalen Benachrichtigung für die Mitarbeiter wird das Ergebnis nur gering „verfälscht“ bzw. die Info wird häufig auch schnell wieder vergessen. Bei einer Erkennung und der Aufklärung ist die Akzeptanz der Mitarbeiter wesentlich höher, als wenn die Mitarbeiter nicht darüber informiert wurden.
- Der Dienstleister versucht die einzelnen Mitarbeiter zu schützen (z. B. im Reporting).
- Personen für bei denen ein Social Engineering-Angriff erfolgreich war, werden aus datenschutzgründen nicht genannt. Allgemein werden keine einzelnen Personen im Bericht benannt.
- Benutzernamen werden ausgegraut – Klarstellung das einzelnen Mitarbeiter nicht schuld sind. Die Informationen werden aufs nötigste Beschränkt.
- Die Ergebnisse werden tlw. auch im Anschluss kommuniziert. Oft werden im Anschluss Awareness-Schulungen mit konkreten Beispielen aus dem Red Teaming gezeigt.
- Es ist nicht das Ziel Ängste von einzelnen Mitarbeitern auszunutzen.
- Es geht nicht darum einzelnen Mitarbeiter bloßzustellen.
- Es darf nicht zum Blamming (Beschuldigung) von einzelnen Mitarbeitern kommen. Der einzelne Mitarbeiter wird beim Test geschützt. Das Social Engineering wird so anonym wie möglich durchgeführt. Es wird nur das notwendigste dargestellt und das es keine Schuld von einzelnen ist. Es geht vielmehr darum, aufzudecken, ob noch weitere Sensibilisierungen notwendig sind.
- Vor dem Exploiten oder ausführen von PoC auf kritischen Systemen wird beim Kunden nachgefragt, ob dies durchgeführt werden kann, ohne dass ein großer Schaden entsteht. Mit eine PoC oder Exploit soll nur gezeigt werden das es funktioniert.
- Normalerweise werden Exploits nur in Testsysteme oder wenn Backups vorhanden sind ausgeführt.
- Es kann viel schief gehen. Dies muss mit dem Kunden abgestimmt sein.
- Red Teaming sollte hoch angesetzt werden, damit dies nicht hochschaukeln.

- Es werden Grenzen einhalten und Exploits nur verwendet, wenn klar ist das ein System nicht abstürzt.
- Produktive System wird sehr vorsichtig vorgegangen. Es reicht ein Connect und das eine Verbindung möglich ist.
- Durch eine Risikoanalyse und eine enge Abstimmung mit dem Kunden werden die Risiken minimiert und mitigiert.
- Bei Fehlern oder Störungen wird der Kunde unterstützt.
- Die Risiken werden durch das Management Größtenteils mitigiert.
- Es wird ein hoher Wert auf Kommunikation gelegt, wo durch Risiken vermindert werden können.
- Es gibt ein Agreement mit dem Unternehmen und die möglichen Risiken werden erläutert. Der Ansprechpartner kann entscheiden, welche Prüfungen sinnvoll sind.
- Es ist noch nie etwas Unvorhersehbares passiert und noch nie zu einem großen Schaden gekommen. Im Zweifel erfolgt eine Abstimmung mit dem Auftraggeber bevor etwas passiert.
- Es werden keine DoS-Angriffe, die die Verfügbarkeit eines IT-Systems gefährdet durchgeführt.
- Es wird im Vorfeld akribisch auf Vorfälle hingewiesen, sodass bspw. Backups und Testsystem bereitgestellt werden.
- Es gab Gespräche mit dem Betriebsrat.
- Es gab bisher keine negativen Erfahrungen im Red Teaming.
- Dadurch das kein blinder, sondern ein sehr konstruktiver Ansatz gefahren wird und der Scope festgelegt wird, kam es nicht zu einem kritischen Ausfall.
- Die Gefahr für einen großen Schaden wird als gering eingestuft, da vor einem Angriff eine Abstimmung mit dem Kunden erfolgt.
- Durch die Tests und aufdecken von Schwachstellen, kommt es zu politischen Streitereien im Unternehmen. Dies kommt, weil ein Abteilungsleiter einer Fertigung andere Ziele und Interessen verfolgt.
- Im Vergleich zu einem realen APT ist ein Red Teaming wesentlich langsamer und vorsichtiger, damit nichts kaputt gemacht wird.
- Es können ordentliche Eskalationswege geschaffen werden, damit kein Schaden entsteht.

Allgemein

- Ein Red Teaming ist rechtlich aufwendig, da Drittpartien beeinträchtigt werden können, wie Cloudprovider, BPO, Hosted Services, etc. Es muss alles rechtlich sauber sein. Der Kunde hat das evtl. nicht auf dem Schirm und haftet am Ende.
- Die Risiken wurden als überschaubar angesehen.
- Risiken nur wenn sie schlecht gemacht sind und auf Seiten des Kunden.
- Ein Red Teaming soll so durchgeführt werden, dass es anschließend wieder im Ursprungszustand zurückgeführt werden kann, dies kann nicht immer gewährleistet werden.

10. Sonstiges - Warum sollte ein Unternehmen Red Teaming bei Ihnen durchführen? Können Sie Referenzkunden nennen, die ein Red Teaming bei Ihnen durchgeführt haben? Welche Kunden führen ein Red Teaming durch?

Warum sollte ein Unternehmen Red Teaming bei Ihnen durchführen?

- Es wird ein konstruktiver Ansatz gewählt. Es wird versucht Dinge vernünftig und richtig zu tun.
- Die Beratung und offene Diskussion mit dem Kunden stehen im Mittelpunkt. Es wird gezielt nach dem was erreicht werden soll und was dafür getan werden muss gefragt.
- Das Unternehmen versucht bei einem Pentesting und Red Teaming nicht nach einem Schema vorzugehen, sondern auf die Bedürfnisse des Kunden einzugehen, die in einem Vorgespräch erörtert werden. Hierbei wird abgestimmt, was das Ziel des Kunden ist, was Teil der Übung und des Projekts ist, was gemacht werden darf und was nicht. Es soll keine Dienstleistung von der Stange sein, sondern ein auf einen Kunden zugeschnittenes Produkt.
- Der Kunde möchte ein Threat Model testen für bestimmte Skills benötigt. Gutes Wissen über Threat Models.
- Es wurde bereits mehrmals genannt, das technische Expertise sehr gut ist, z. B. beim Exploiting.
- Der Dienstleister ist sehr breit aufgestellt bei bestimmten Security-Themen.
- Das Unternehmen weist eine große Erfahrung auf und ist beteiligt an Standards.
- Konzentration auf die Bereiche Penetrationstests und Red Teaming.
- Das Unternehmen möchte die Anforderungen des Kunden erfüllen. Dabei wird großer Wert auf eine klare Kommunikation gelegt. Wenn das Unternehmen keine Expertise in einem bestimmten Bereich hat wird ein Kunde auch weitergegeben.
- Das Unternehmen ist sehr stark im Bereich ISMS, ISO 27001 und IT-Grundschutz und kann daher sehr gut die Verbindung zwischen ISM und Red Teaming darstellen. Dies bietet große Vorteile für den Kunden.
- Das Unternehmen macht bereits vielen Jahren Penetrationstests und ein umfangreiches Wissen ist bereits vorhanden.
- Mit dem Thema Red Teaming hat man sich bereits rechtzeitig beschäftig und konnte schon viel Erfahrung sammeln.
- Das Unternehmen gehört zu den größten Sicherheitsdienstleistern in Deutschland.
- Das Unternehmen hat einen sehr breiten Wissensschatz und Erfahrung im Unternehmen
- Ist bereits sehr lange im Security-Bereich auf dem Markt.
- Das Unternehmen hat Teams, die auf unterschiedliche Themenbereiche spezialisiert sind (Windows, SAP, Mobile, usw.). Es können somit Experten aus unterschiedlichen Bereichen, bei verschiedenen Anwendungsfällen hinzugezogen werden.
- Es gibt auch eine interne Forensik die auch Workshops für eine Forensik-Abteilungen in einem Unternehmen anbieten, um Detektierungsmaßnahmen einzurichten und Angriffe besser erkennen zu können.

- Es werden keine Produkte, sondern nur Dienstleistung und Know-how verkauft.
- Das Unternehmen hat eine sehr große Kompetenz. Es beschäftigen sich sehr viele Mitarbeiter mit IT-Sicherheit und es gibt einen sehr großen Austausch untereinander.

Können Sie Referenzkunden nennen, die ein Red Teaming bei Ihnen durchgeführt haben?

- Es wurden keine Referenzkunden genannt.

Welche Kunden führen Red Teaming durch?

- Es gibt aktuell nur wenige Kunden, die ein Red Teaming durchführen.
- Breite Bereiche
- Durchgemischte Branchenvielfalt, deutsche und internationale Kunde
- Der Kundenkreis kann keiner festen Branche zugeordnet werden.
- Der Kundenkreis kommt aus dem Health-Care-Bereich (Krankenhäuser), Energiesektor, Finanzsektor und produzierenden Gewerbe. Der Kundenkreis ist breit verteilt.
- Nachfrage kommt hauptsächlich aus der Finanzbranche und eher von großen Unternehmen und mit hohem Reifegrad.
- Red Teaming ist vor allem im Bankensektor gefragt.
- Das Red Teaming wird im Bankensektor durchgeführt, da es dort viele national als auch internationale Regularien gibt.
- Es gibt Banken die aktuell Red Teams im Unternehmen aufbauen.
- Red Teaming wird häufig in hochregulierten Bereichen wie dem Finanzsektor durchgeführt.
- Die Banken werden dabei unterstützt ein Red Teaming nach dem TIBER-EU Framework durchzuführen und aufzubauen.
- Die meisten Kunden die Red Teaming beauftragen kommen aus der Finanzwelt/ Bankenindustrie (Frankfurt). Die Anforderungen kommen auch aus diesem Bereich.
- Red Teaming wurde in großen Konzernstruktur, einem Krankenhaus und einem Recycling-Unternehmen durchgeführt.
- Viele Kunden kommen aus dem KRITIS-Bereich.
- Die Kunden liegen in Finanzsektor und der Pharmazie.
- Das Unternehmen führt Red Teaming zu 80 % bei Banken durch. Weitere Bereiche sind Versicherung und Pharma.
- Weitere Bereiche sind Regierungsorganisationen, kritische Infrastrukturen und die Automobilindustrie
- Große Kunde
- Projekte wurden nur bei wenigen großen Unternehmen durchgeführt.
- Hauptsächlich bei großen Institutionen und Konzerne, die das Budget aufbringen können.
- Ein Red Teaming wird in der Regel von großen Konzernen durchgeführt, die bereits einen bestimmten Reifegrad erreicht haben.

- Der Kundengreis ist ab deutschen Mittelstand und aufwärts. Teilweise auch kleine Unternehmen („Hidden Champions“) und öffentliche Bereiche.
- Die meisten Kunden kommen aus dem Mittelstand. Hier wird meistens die Ausprägung Innentäter oder Sabotage von bestimmten Assets gewählt.
- Vereinzelt wurden auch Red Teaming bei kleinen Unternehmen durchgeführt
- Es gibt nur selten Aufträge von kleinen Unternehmen, da dies häufig noch nicht darauf vorbereitet sind. Bei diesen kommen eher Aufträge im ISMS oder Pentest-Bereich.
- Es wurden bisher nur Projekte auf nationaler Ebene durchgeführt.

Sonstiges

- Es ist aktuell keine Akquise notwendig, da die Aufträge von den Unternehmen automatisch kommt aufgrund der guten Reputation.
- Es wird bisher keine aktive Akquise zum Thema Red Teaming, da die Kunden das Unternehmen bereits vom Pentesting kennen.
- Red Teaming ist aktuell ein Paradigmenwechsel und in der Entwicklungsphase. Es wird sich noch weiterentwickeln und auf die Gegebenheiten anpassen

Anlage 4 Interviewprotokoll Auftraggeber

1. Warum wurde ein Red Teaming durchgeführt? Welches Ziel/e sollte mit Red Teaming erreicht werden?

Warum wurde ein Red Teaming durchgeführt?

- Oft geht es darum politisch im Unternehmen voranzukommen und Entscheidungen durch Beweise zu erzwingen.
- Es wurde geprüft, ob ein bestimmter Angriff erkannt werden.
- Es wird geprüft, ob bestimmte simulierte TTPs erkannt werden.
- Es wird versucht bekannte Schwachstellen auszunutzen und zu prüfen, was durch diese Schwachstellen möglich ist.
- Im Sicherheitsbereich gibt es ein allgemeines Ressourcenproblem. Es gibt Schwachstellen, die bereits bekannt sind, damit diese behandelt werden muss die Schwachstelle bewiesen werden.
- Bei der Organisation werden sowohl Schwachstellenanalyse mit Audits und Penetrationstests als auch Red Teaming. Red Teaming wird als Ergänzung zum White-Box-Test gesehen. Red Teaming wird als Black-Box-Test durchgeführt, d.
- h. das Red Team hat, wie ein realer Angreifer, keine Informationen. Es soll dabei helfen „blinde Flecken“ aufzudecken. Zudem ist es ein Training für das Red als auch das Blue Team.
- Das White Team wird über den Test informiert und ist in Kommunikation mit dem Red Team. Es erfolgen Abstimmungen nach jeder Stufe. So können die Vorteile von einem Black-Box und White-Box-Test kombiniert werden.
- Es kann helfen die Denkweise des Vorgesetzten zu ändern. Die Denkweise ist häufig, dass durch den Kauf eines Security-Produkts ein ausreichender Schutz vorhanden ist. Red Teaming hilft dabei, die Mitarbeiter von etwas anderem zu überzeugen.

Welches Ziel/e sollte mit Red Teaming erreicht werden?

- Ziel ist es in der Regel von außen Zugang zum Netzwerk zu erhalten und anschließend zu prüfen, ob eine Rechte Eskalation möglich ist. Es soll getestet werden, wie weit das Red Team kommt.
- Neben technische Schwachstellen sollen vor allem die Prozesse und die Kommunikation bei einem Sicherheitsvorfall überprüft werden.
- Das Funktionieren der geplanten Vorgehensweisen bei einem Angriff wird getestet.
- Die Incident Response Möglichkeiten und Prozesse werden durch den Test überprüft.
- Der Schwerpunkt beim Red Teaming liegt auf technische Schwachstellen. Phishing wird in einer separaten Kampagne eingesetzt.
- Beim Red Teaming geht es um das Erkennen von Angriffen.

- Ziele in einem Red Teaming bei einer Bank können Kundendaten oder der Zahlungsverkehr sein.
- Beim Red Teaming wird ein Ziel festgelegt und häufig wird nur nach einem Weg gesucht.
- Das Ziel ist es, egal auf welche Art und Weise, das Ziel zu erreichen.

2. Was hat Red Teaming bewirkt (Vorteile/ Nutzen / Mehrwert)? Warum sollten ein Unternehmen ein Red Teaming durchführen? Werden weitere Red Teaming Projekte durchgeführt?

- Die gefunden Schwachstellen werden behoben und nachgeprüft.
- Durch Red Teaming wurden Prozesse optimiert und Schwachstellen behoben.
- Es wurden auch Server gefunden, auf denen bereits ein unbekannter Benutzer angemeldet war und somit auch geprüft, wie man mit dieser Situation umgeht.
- Durch den Red Teaming Report hat man Beweise, Nachweise und Fakten über bestimmte Sicherheitsmängel. Diese können genutzt werden, um auf verantwortliche Personen zuzugehen und bewirken, dass etwas gemacht wird. Häufig müssen Patches eingespielt oder Konfigurationen angepasst werden. Man hat dadurch einen Nachweis, was alles schief gehen kann. Durch geschaffene Fakten ist es schwierig dagegen zu argumentieren.
- Ein Red Teaming ist realitätsnaher als ein Penetrationstests.
- Beim Blue Team wird hinterfragt, ob Alerts aufgetaucht sind, diese bearbeitet oder ignoriert wurden. Gibt es Server, die nicht geloggt werden?
- Der Haupttreiber von Red Teaming ist den Stand der Erkennungs- und Reaktionsfähigkeit zu prüfen. Wie gut und wie schnell ist diese?
- Nach einem Red Teaming kann herausgefunden werden, wie ein Angriff hätte verhindert werden können und welche Maßnahmen notwendig sind.

3. Hatte die Durchführung negative Auswirkungen? Ist durch das Red Teaming ein Schaden entstanden?

- Das ISMS ist sehr detailliert beschrieben. Dadurch sind nicht alle Prozesse bekannt und es kann zu Problemen kommen.
- Das Red Team hat noch nichts kaputt gemacht.
- Es kam schon zu Fehlreaktionen der Verteidigung, die aus gutem Glauben eine falsche Entscheidung getroffen haben. Dies hatte eine Auswirkung auf die Verfügbarkeit.
- Keine negativen Erfahrungen mit Social Engineering.
- Es gab keine negativen Auswirkungen.
- Es gab in den USA ein Fall, bei dem ein Angriff in den Nachrichten veröffentlich wurde, der eigentlich ein Red Teaming war.

4. Welcher Dienstleister wurde ausgewählt? Wie wurde der Dienstleister ausgewählt? Waren Sie mit dem Ergebnis zufrieden?

- Das Red Team gehört zur Organisation und es wird kein externer Dienstleister benötigt
- Das Unternehmen ist zufrieden mit den Ergebnissen mit dem Dienstleister.
- Es konnte keine Aussage über die Auswahl des Dienstleisters getroffen werden.